ATAIS - Response Plan



Advanced Threat Analytics Implementation Services

Preparado para

[Customer]

9/19/2016

Versión 1 Draft

Preparado por

**[Type Author Here]**

[Type Author Position Here]

[Type Author Email Here]

Contribuidores

**[Type Contributors Here]**

Revisión y hoja de firmas

Control de cambios

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha | Autor | Versión | Descripción del cambio |
|  |  | 1 | Borrador inicial para revisión/discusión |
|  |  |  |  |
|  |  |  |  |

Revisores

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | Versión aprobada | Posición | Fecha |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabla de Contenidos

[1 Introducción 7](#_Toc462266268)

[2 Cómo utilizar este plan 8](#_Toc462266269)

[3 Roles y responsabilidades 9](#_Toc462266270)

[4 Proceso de respuesta a incidentes de seguridad 12](#_Toc462266271)

[4.1 Evaluación 13](#_Toc462266272)

[4.1.1 Diagnóstico 13](#_Toc462266273)

[4.1.2 Clasificar 14](#_Toc462266274)

[4.1.3 Incidentes Graves 18](#_Toc462266275)

[4.2 Preparar 20](#_Toc462266276)

[4.2.1 Priorizar 20](#_Toc462266277)

[4.2.2 RACI 21](#_Toc462266278)

[4.2.3 Agendamiento 21](#_Toc462266279)

[4.3 Comunicar 22](#_Toc462266280)

[4.3.1 Comunicaciones Ejecutivas e Informes 22](#_Toc462266281)

[4.3.2 Declaración de Violación 23](#_Toc462266282)

[4.3.3 Comunicaciones Externas 24](#_Toc462266283)

[4.3.4 Comunicaciones Internas 25](#_Toc462266284)

[4.4 Responder 25](#_Toc462266285)

[4.4.1 Investigar 25](#_Toc462266286)

[4.4.2 Contención 29](#_Toc462266287)

[4.4.3 Erradicación 30](#_Toc462266288)

[4.4.4 Recuperación 32](#_Toc462266289)

[4.5 Cierre 34](#_Toc462266290)

[4.5.1 Post mortem 34](#_Toc462266291)

[4.5.2 Documentación 35](#_Toc462266292)

[4.5.3 Mejora del Proceso 35](#_Toc462266293)

[5 Apendice: Lectura Adicional 36](#_Toc462266294)

We are very interested in your input!  If you have comments or would like to request an update to this document, please provide your feedback to the [SDM Suggestions alias](mailto:msdmods@microsoft.com).   Attach the document and clearly describe the changes you would like and explain why the changes are needed.

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click on File
2. Click on the Options on the left
3. Click on Proofing
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl H to open the Find and Replace box
2. Make sure your cursor is in the ‘Find what’ box.
3. Click on the More button at the bottom left
4. Click on the Format Button at the bottom left and select Style
5. Scroll down, locate select the “Visible Guidance”
6. Make sure the ‘Replace with’ box is empty:
7. Click ‘Replace All”
8. If not empty - click on the format button in the lower left hand corner. Scroll down and chose ‘(no style)’then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

Template Guidance

Description:

1. Introducción

**Section Detail:** This section should provide the purpose of this response plan, any initiation guidelines, how to use this plan, detail on the contents of the document and the scope of this documents use.

Todos los miembros del ambiente TI deberían estar conscientes de que hacer en el caso de incidente. El equipo de Respuesta a Incidentes de Seguridad (SIR) realizará la mayoría de las acciones en respuesta a un incidente, pero todos los niveles del personal de TI deberían estar instruidos de cómo informar los incidentes internamente. Los usuarios finales deberían reportas actividades sospechosas al personal TI directamente o a través de la mesa de ayuda, en vez de hacerlo directamente al SIR.

Cada miembro del equipo debería revisar el plan de respuesta a incidentes detalladamente. Tener disponible el plan para todos los miembros de TI, asegurará que, en caso de incidente, se apliquen los procedimientos correctos.

1. Cómo utilizar este plan

**Section Detail:** This section should contain an explanation of the different levels of incident response in relation to ATA findings and corresponding escalation points. It should also provide detail regarding how this document should be used for each part of the response process.

Este documento describe los procedimientos operativos estándar de como el equipo de Respuesta a Incidentes de Seguridad (SIR), en conjunto con otros equipos de operación, responderá a los eventos que sean detectados por la solución Microsoft Advanced Threat Analytics (ATA). Este documento NO explicará en detalle los procedimientos de Respuesta a Violaciones de Seguridad y escenarios de remediación, salvo ocasionales referencias definidas en el alcance.

Se debe tener en cuenta que los pasos descritos en este plan no son secuenciales. Por el contrario, ocurren durante todo el incidente. Por ejemplo, la documentación comienza al principio del incidente y continúa a lo largo del ciclo de vida del mismo. Lo mismo sucede con la comunicación.

Otros aspectos del proceso trabajaran uno al lado del otro. Por ejemplo, como parte de la evaluación inicial, se puede tener una idea de la naturaleza del ataque. Es importante usar esta información para contener el daño y minimizar el riesgo tan pronto como sea posible. Si se actúa rápido, se puede ahorrar tiempo y dinero y conservar la reputación de la compañía.

Sin embargo, hasta que se entienda el tipo y la severidad del compromiso en detalle, no se puede ser capaz de contener el daño y minimizar el riesgo efectivamente. Una respuesta entusiasta podría incluso causar más daño que el ataque inicial. Al trabajar estos pasos uno junto al otro, se conseguirá el mejor compromiso entre una acción rápida y eficaz.

**Nota:**Es muy importante probar minuciosamente el proceso de respuesta a incidentes antes que ocurra un incidente. Sin pruebas exhaustivas, no se puede estar confiado en las medidas que se implementaron serán efectivas para responder a los incidentes. Se debe pensar de manera similar a un plan de recuperación de desastres. Los planes de recuperación de desastres a menudo son probados para asegurarse que un *datacenter* secundario funciona en caso de un evento. Se debería probar el proceso documentado dentro de este documento de una forma similar. Utilizando ejercicios de simulación, donde se recorren los pasos de un incidente, es una manera muy efectiva para validar procesos y procedimientos.

1. Roles y responsabilidades

**Section Details:** This section is where we will provide a template for the incident response team at the customer and potentially how Microsoft fits into that. Theory is that this section becomes a template which is filled in as a result of the response planning workshop activity.

**Instruction:** Please update the following table to include members from your customer that will be included within each role. This table does not need to list a specific individual. A team name will suffice.

En la siguiente tabla se destacan los roles y responsabilidades que han sido identificados como parte del proceso de Respuesta a Incidentes de Seguridad. Esos roles y responsabilidades identifican quién debe ser involucrado y cuáles son sus responsabilidades durante un incidente.

|  |  |  |
| --- | --- | --- |
| **Posible Nombre de Rol** | **Responsabilidades/Competencias** | **Miembros de la Organización** |
| EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD (SIR) | * Dueño de la respuesta a incidentes * Realizan el diagnostico/evaluación/clasificación inicial de seguridad * Entrega el resumen ejecutivo (comunicación) * Establecen los canales y objetivos de comunicación apropiados * Coordina las actividades de análisis con los equipos de operaciones y expertos en la materia   + Investigar   + Contener   + Erradicar   + Recuperar * Cierre   + Post Mortem   + Documentación   + Mejora del Proceso |  |
| GESTOR DEL INCIDENTE  (ASIGNADO POR EL SIR) | * Ejecutar la coordinación de actividades para el equipo SIR * Administrar el incidente a través de las actividades del ciclo de vida * Punto de decisión para el equipo SIR |  |
| GESTOR DE COMUNICACIONES | * Dueño de los flujos de comunicación para la respuesta del incidente * Se comunica con las Gerencias/Jefaturas para determinar los canales y objetivos de comunicación |  |
| CONTACTOS OPERACIONES/TI | * Detecta posibles vulnerabilidades (monitoreadas por ATA) * Realiza la evaluación inicial basada en la guía de la herramienta y la capacitación que posean * Moviliza los recursos que puedan:   + Analizar las alertas de Seguridad generadas por ATA y otras Fuentes   + Diagnosticar alertas para revisar la validez, alcance e impacto de seguridad * Escalar incidentes de seguridad al equipo SIR para garantizar una investigación más amplia de seguridad * Movilizar recursos clave desde ingeniería, comunicaciones, operaciones y legal sobre el principio de “necesidad de saber” (NTK) para agilizar el proceso de investigación * Proveer asistencia al equipo SIR en la obtención de pruebas, conducir la investigación forense. Analizar la causa raíz y revisar minuciosamente el alcance e impacto del incidente * Diseñar, priorizar e implementar capacidades de remediación y planes dentro del ambiente, además de conducir procesos y mejoras técnicas basadas en las recomendaciones post mortem del incidente * Administrar los cambios a la configuración relevantes para la seguridad como parte del proceso de administración de cambios |  |
| EXPERTOS EN LA MATERIA | Dependiendo de la naturaleza del incidente, el equipo SIR y los equipos de operaciones podrías contratar Expertos en la Materia desde organizaciones internas o externas para asistencia en la investigación |  |
| REPRESENTANTE LEGAL | * Representación legal familiarizada con las políticas de respuesta a incidentes establecidas * Determina como proceder durante un incidente con mínima responsabilidad legal y máxima habilidad para procesar a los delincuentes * Coordinar todas las comunicaciones para aplicar la ley externa o a las agencias investigativas externas   Nota: Antes que un incidente ocurra, el Representante Legal debería tener injerencia sobre las políticas de monitoreo y respuesta para asegurar que la organización no se está poniendo en riesgo legal durante una operación de limpieza o contención. Es muy importante considerar las implicaciones legales de apagar un sistema potencialmente violando los acuerdos de nivel de Servicio (SLA) o acuerdos de adhesión con los clientes, o no apagar un Sistema comprometido y ser responsable por los daños causados por los ataques enviados a ese sistema. |  |
| GERENCIA/JEFATURAS | * Aprobar y dirigir la política de seguridad * Determinar el impacto total (financiero y de otros tipos) del incidente en la organización * Guía la comunicación en lo referente a cuál información debería ser revelada en los medios * Determina el nivel de interacción entre el representante legal y los organismos encargados de hacer cumplir la ley   Nota: Dependiendo de un incidente particular, se podría involucrar solo gerentes departamentales o gerentes de toda la organización. Los gerentes apropiados variarán según sea el impacto, ubicación, severidad y tipo de incidente. |  |

1. Proceso de respuesta a incidentes de seguridad

El proceso de respuesta a incidentes de seguridad comienza con el diagnóstico inicial para determinar la validez, alcance e impacto. Una vez que se determina que el incidente es relativo a seguridad y han sido evaluados su alcance, impacto y severidad, se debe garantizar la investigación. El proceso investigativo, conducido por los equipos de SIR y operaciones, obtendrán la evidencia, conducirán el análisis forense e intentarán determinar la causa raíz. Además, el alcance, impacto y severidad seguirán siendo evaluadas continuamente a través de la investigación, los impactos de cumplimiento y privacidad también serán determinados. El resultado de este proceso de investigativo será la clasificación del incidente, seguido por una guía prescriptiva de las acciones a seguir en cada tipo de clasificación de incidente. El proceso está representado gráficamente en la figura 1:

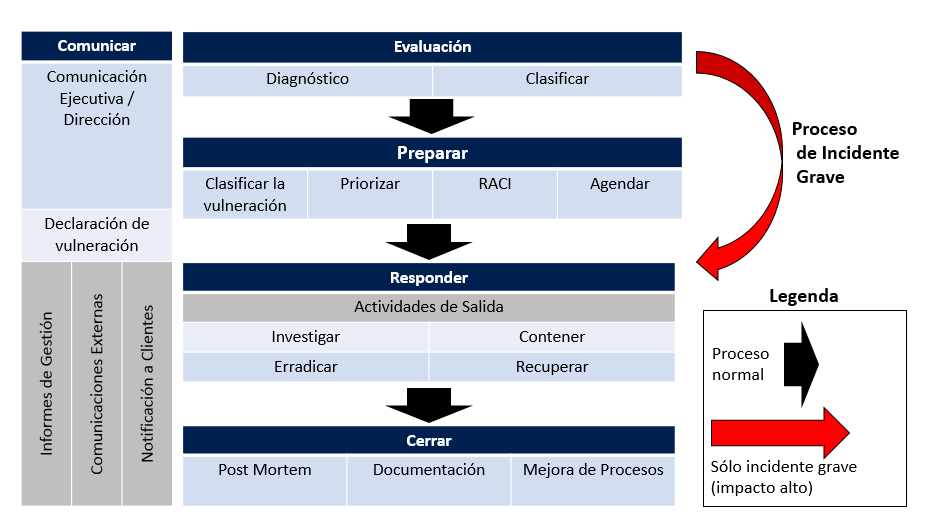


Figura 1 Proceso de Respuesta a Incidente de Seguridad

Las siguientes subsecciones describen cada una de las fases del proceso con más detalle.

* 1. Evaluación
     1. Diagnóstico

Cada escalamiento puede no ser un incidente de seguridad, operaciones debe realizar actividades de diagnóstico para examinar cada escalamiento y hacer una determinación de cuando está ocurriendo un incidente de seguridad. Numerosas actividades pueden ser incluidas en el proceso de administración de incidentes, comenzando por el diagnóstico del incidente para identificar qué situación se está enfrentando.

Los equipos de operaciones deberían diagnosticar un incidente antes de escalarlo a SIR. Una vez que el incidente está escalado, el equipo SIR conducirá una revisión preliminar del escalamiento por medio de artefactos técnicos para obtener conocimiento de la información. Los aspectos claves a considerar durante esta fase serán los antecedentes del incidente y el alcance. Las siguientes tablas indican las preguntas frecuentes que se hacen para evaluar el incidente.

|  |
| --- |
| **Antecedentes del Incidente** |
| ¿Cuál es la naturaleza del problema, según lo que se ha observado ahora? |
| ¿Cuál fue el problema detectado inicialmente? ¿Qué fue detectado y por quién o cuál sistema? |
| ¿Qué componentes de la infraestructura de Seguridad existen en el ambiente afectado? (ej. firewall, anti-virus, etc.) |
| ¿Cuál es la relación con seguridad de los componentes de infraestructura TI afectados? ¿Qué tan reciente, si es que se ha realizado, se hizo una evaluación de vulnerabilidades? |
| ¿Qué grupos u organizaciones fueron afectados por el incidente? ¿Ellos saben del incidente? |
| ¿Dónde fueron observados otros incidentes de seguridad en el ambiente afectado o en la organización recientemente? |

|  |
| --- |
| **Alcance del Incidente** |
| ¿Quién fue designado como el gestor del incidente? |
| ¿Qué componentes de infraestructura TI (controladores de dominio de Active Directory Domain Services, credenciales altamente sensibles, servidores, sitios web, redes, etc.) están afectados directamente por el incidente? |
| ¿Cuáles aplicaciones y procesos de datos hacen uso de los componentes de infraestructura TI afectados? |
| ¿Se conoce el cumplimiento u obligaciones legales vinculadas al incidente (ej. PCI, leyes de notificación de vulnerabilidades, etc.)? |
| ¿Cuáles son los puntos de ingreso y egreso posibles para el ambiente afectado? |
| ¿Qué teorías iniciales existen de cómo ocurrió el compromiso? |
| ¿La infraestructura afectada representa amenazas para otras organizaciones? |

Modificado desde: <https://zeltser.com/security-incident-questionnaire-cheat-sheet/>

|  |
| --- |
| **Consideraciones de Comunicaciones** |
| ¿Quién fue designado como gestor de comunicaciones? |
| ¿Qué personas saben del incidente? ¿Cuáles son sus nombres y afiliación al grupo o a la compañía? |
| ¿Qué ejecutivo necesita ser contactado primero, para notificación y dirección? |
| ¿Qué mecanismos utilizará el equipo para comunicarse mientras administra el incidente (ej. mail, conference call, etc.)? ¿Qué capacidades de encriptación deberían ser usadas? |
| ¿Cuál es el periodo interno de reporte de actualizaciones? ¿Quién es el responsable de eso? |
| ¿Existe un consejero externo para guiar en las comunicaciones internas a los empleados o externa a los clientes o proveedores? |
| ¿Qué debería ser compartido y este mensaje ayudará a la situación o será una causa potencial de un daño adicional a la reputación? |

|  |
| --- |
| **Otras consideraciones** |
| ¿Este evento ha ocurrido y ha sido resuelto anteriormente? ¿Existe documentación de referencia? |
| ¿Se sabe si existen factores atenuantes del riesgo? |
| ¿Se sabe si existen contingencias? |
| ¿Quién está autorizado para tomar decisiones de negocio con respecto a las operaciones afectadas? |
| ¿Se está utilizando un sitio de colaboración? ¿Está aislado y seguro? ¿Se deben proteger todos los datos que están siendo usados para la respuesta? |
| ¿Quién llevará a cabo la examinación en terreno de la infraestructura TI afectada? Anote su nombre, cargo, teléfono, y correo. |

Modificado desde: <https://zeltser.com/security-incident-questionnaire-cheat-sheet/>

* + 1. Clasificar

Un incidente de seguridad debe ser clasificado para asignar el nivel de respuesta requerido por ese incidente, para identificar apropiadamente recursos para la respuesta y para establecer una línea de tiempo de acciones basado en los acuerdos y clasificaciones de [Customer]. Por último, la clasificación relaciona específicamente el riesgo que le incidente tiene en el negocio. El equipo SIR, en consulta con los equipos de operaciones, clasificará el incidente de seguridad y asignará un nivel de severidad basado en las piezas afectadas y el impacto asociado con ellas.

La siguiente tabla muestra un ejemplo de severidades y naturaleza de compromisos. El equipo SIR debería actualizar esas severidades y, si es necesario, agregar nuevas definiciones basadas en sus propios requerimientos y la interpretación de cuál es el impacto para el negocio

Note: Consultants should help guide customers through the process of classifying a security incident, using the table below. Customers should think through these levels and provide business impacting scenarios updating the definitions to be more relevant to their organization.

|  |  |
| --- | --- |
| Severidad | Naturaleza del Compromiso |
| Crítica  Sev 0 | Alteración o divulgación de datos HBI, denegación de servicio cruzado, elevación de privilegios en el sistema para procesar datos HBI, elevación del administrador de servicio o elevación de privilegio *cross-tenant*, intento de extracción exitosa o sospechosa de credenciales o HBI. |
| Alta  Sev 1 | Suplantación de identidad, manipulación de MBI/LBI/PII, manipulación de auditoría, divulgación de MBI/PII, Denegación de Servicio, elevación de privilegio sobre un Sistema que NO maneja HBI o intentos de extracción exitosa o sospechosa de datos no sensitivos. |
| Media Sev 2 | Suplantación de identidad con la necesidad de intervención del usuario, moderada manipulación de auditoria, divulgación de LBI o sistema de información interno, Denegación de Servicio limitada, compromiso de activo que puede dar acceso a HBI/MBI. |
| Baja  Sev 3 | El adversario está realizando reconocimiento contra un servidor o servicio o intentos no exitosos para obtener acceso a HBI/MBI/PII |

* + - 1. Clasificación de ATA de Actividades Sospechosas

Microsoft Advanced Threat Analytics (ATA) se enfoca en detector una variedad de amenazas relacionado con las credenciales del Active Directory Domain Service. ATA categoriza esas amenazas de la siguiente manera:

* **Ataques Maliciosos** – detección de ataques maliciosos conocidos a través de los patrones que los atacantes usan para obtener control de las credenciales valiosas dentro de su organización
* **Riesgos e Incidentes de Seguridad Conocidos** – detección de incidentes de seguridad conocidos y riesgos que pudieran ser relevantes en el ambiente y potencialmente abrir la posibilidad de compromiso

**Comportamiento anormal** – el análisis de comportamiento descubre actividades sospechosas y comportamiento anormal, aprovecha *machine learning* (análisis de comportamiento de usuarios y entidades) para identificar patrones y alertar sobre anomalías descubiertas.

Por defecto, *Microsoft Advanced Threat Analytics* entrega una severidad técnica a cada actividad que reporta. Esas clasificaciones deberían ser consideradas como un punto inicial para la revisión del incidente. Sin embargo, dependiendo de la naturaleza del evento que esté siendo observado, el eventual riesgo para la organización podría variar dependiendo del impacto en el negocio de la actividad sospechosa identificada.

Por ejemplo, ATA podría reportar un “Golden Ticket” con una severidad “media”. Sin embargo, después de una investigación exhaustiva, el equipo SIR identifica que el incidente es real y la severidad es “alta” debido a que ahora el atacante tiene la habilidad de actuar como controlador de dominio dentro del ambiente. Mientras que ATA configura esta alerta como “media” por defecto, la clasificación de la organización debería ser “Critica Sev 0” con un alto impacto en el negocio.

Si ATA identifica un incidente, se debe considerar lo siguiente:

1. ¿Está aislado el incidente o existen múltiples actividades sospechosas relacionadas?
2. ¿Cuál es la sensibilidad o valor de las entidades que están siendo atacadas?
3. ¿Las cuentas o equipos en cuestión, son utilizados para actividades administrativas?

Se debe tener en cuenta que sólo una porque una cuenta que haya sido atacada no tenga el carácter administrativo, no significa que el incidente no tenga una severidad alta. Mientras que el compromiso de una cuenta con privilegios administrativos es “crítica”, un usuario regular podría también ser crítico dependiendo del acceso que el usuario tenga. Si se considera por ejemplo la severidad de que el objetivo sea la cuenta del Gerente de Finanzas. Esa cuanta podría ser regular, sin accesos administrativos, pero podría tener acceso a información altamente sensible, lo que resultaría en una severidad crítica.

**Instructions:** During the “Event Definition and Risk Classification” workshop, you guided your customer through defining the severity of each of the ATA event definitions along with conditions that may drive that severity rating. Update the following table to reflect decisions that were made in that workshop.

La siguiente tabla provee un listado de cada actividad sospechosas que ATA puede identificar en el ambiente. Durante los talleres de plan de respuesta, la clasificación de riesgo del negocio fue definida por cada actividad sospechosa con las condiciones que se aplican, o podrían alterar, la severidad definida. Se debe aprovechar esa información como punto de partida cuando se empieza la clasificación de riesgo para las actividades sospechosas que ATA puede encontrar.

|  |  |  |  |
| --- | --- | --- | --- |
| Actividad Sospechosa de ATA | Severidad ATA | Clasificación de riesgo | ¿Por qué’? ¿Bajo qué condiciones? |
| Reconocimiento usando DNS | Medio | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Reconocimiento usando Enumeración de Cuenta | Medio | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Reconocimiento usando Fuerza Bruta (LDAP, Kerberos) | Medio | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Reconocimiento usando Enumeración de Sesión SMB | Medio | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Pass-the-Ticket | Alto | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Pass-the-Hash | Alto | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Over-Pass-the-Hash | Alto | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Malware Skeleton Key | Alto | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Forged PAC | Alto | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Golden Ticket | Medio | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Ejecución Remota | Bajo | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Replicación Maliciosa de Servicios de Directorio | Medio | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Requerimiento malicioso de Información privada de Protección de datos | Alto | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Comportamiento anormal basado en autenticación, autorizacion y horas de trabajo | Medio (Alto si es cuenta Admin) | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Borrado masivo de objetos | Medio | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Cuentas sensitivas expuestas en autenticación de texto plano | Bajo | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Servicio exponiendo autenticación de cuentas en texto plano | Bajo | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Implementación de protocolo inusual | Medio | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Detección de la vulnerabilidad MS11-013 | Medio | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Confianza rota | Bajo | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |
| Uso de la cuenta Honey Token | Bajo | <Ingrese la Clasificación de Riesgo aquí> | <Ingrese el racionamiento condicional para configurar, clasificar o ajustar aquí> |

* + 1. Incidentes Graves

Como se indica en la sección de este documento “Como usar este plan”, las actividades realizadas en esas fases podrían ocurrir en paralelo según sea la severidad y prioridad de las acciones. En el caso de un incidente de alta severidad, las acciones para comunicar y contener tomarán precedencia sobre las actividades como agendar, RACI e incluso la erradicación.

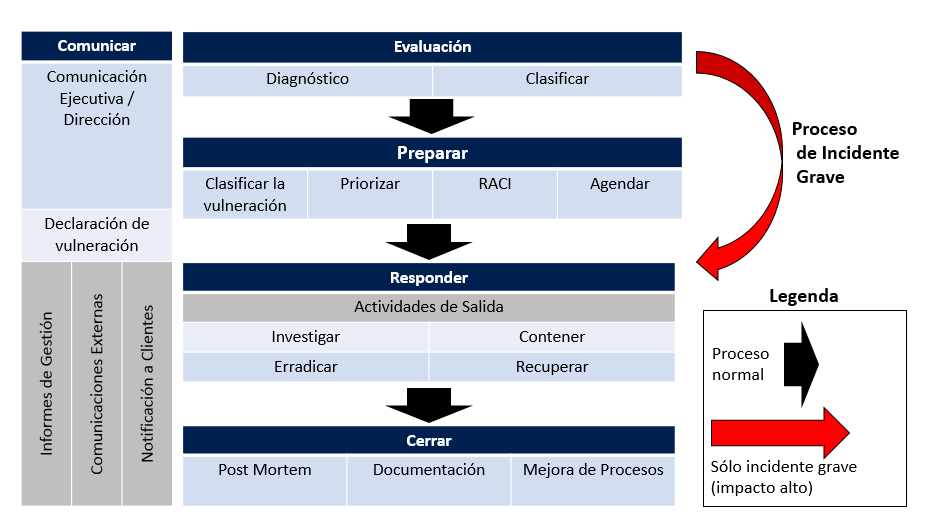


Figure 2 – Flujo de Incidentes Graves

En casos como este, es bueno tener a mano un plan de batalla. A continuación, se muestra un ejemplo de un plan de batalla sobre un incidente de alta severidad que podría ayudar como guía en el proceso de un incidente grave y proveer con enlaces directos a los procedimientos estándar operativos (SOP). Esos SOP deberían estar fácilmente disponibles para todo el equipo de operaciones durante un evento.

**Note:** Consultants should work with key stakeholders to populate the table found below with document links and names of individuals accountable for each activity

|  |  |  |
| --- | --- | --- |
| ACTION | ¿Cómo hacerlo? (SOP) | Contacto |
| Clasificación y priorización rápida |  |  |
| Proceso de notificación a ejecutivos |  |  |
| Investigación y contención rápida |  |  |
| Notificación rápida a PR/LEGAL/ETC |  |  |
| Iniciar revisión de RACI y agendamiento |  |  |

* 1. Preparar
     1. Priorizar

Priorizar llama al orden. Si dos eventos Sev 0 ocurren, ¿cuál debería ser atendido primero? También, los objetivos y las actividades necesarias para atender un evento deben ser priorizadas.

Antes de que una respuesta apropiada a un incidente de seguridad pueda ser definido, el equipo debe tener un entendimiento acabado de las prioridades de respuesta. Esas podrían variar, de acorde con los factores específicos organizaciones o del incidente.

Ejemplo de escenario de priorización:

* Si un adversario es capaz de comprometer un activo que impactará en las licencias del cliente, la prioridad más alta debería ser la integridad del sistema
* Si el sistema comprometido es utilizado para almacenar PII de clientes, la más alta prioridad podría ser identificar el grado de acceso no autorizado a las fuentes de datos dependiendo del contexto.
* Si el sistema comprometido se utiliza para la prestación de servicios de autenticaciones, la restauración confiable del servicio podría ser la prioridad más alta

Las prioridades normalmente son decididas por el Gestor de Incidentes con la dirección de, posiblemente, todos los otros roles. La adjudicación por jefaturas/gerencia puede ser necesaria y puede involucrar un patrocinador ejecutivo desde la unidad de directorio impactada directamente.

Un ejemplo de lista de prioridades para un incidente de Seguridad que involucre una extracción de datos de cliente, puede ser similar a lo siguiente:

|  |  |
| --- | --- |
| Elemento de éxito | Prioridad (siendo 1 alta y 6 baja) |
| Minimizar el impacto al cliente | 1 |
| Ejecutar acciones de remediación | 2 |
| Restaurar las operaciones rápidamente | 3 |
| Dirección de riesgo legal o regulatorio | 4 |
| Cobertura de medios | 5 |
| Identificar actores involucrados en la brecha | 6 |

Note: As previously stated, priorities and success elements will vary based on the severity and business impact of the security incident. Consultants should work with customers to define a list of Success Elements for most security incidents and prioritize them during the Prepare phase, and continue to revisit throughout the incident lifecycle.

* + 1. RACI

Una vez que las prioridades han sido establecidas y acordadas, el siguiente paso es identificar las tareas que están involucradas en ejecutar esos procesos, identificar a los individuos que serán dueños de completar esas tareas y verificar cualquier redundancia. Responsable, A cargo, Consultado e Informado (matriz RACI) son herramientas utilizadas para asegurar que actividades importantes no son pasadas por alto o duplicadas. Esos roles podrían variar o depender del incidente. Completando una matriz RACI debería ocurrir cada vez que el proceso es invocado.

El siguiente es un ejemplo de matriz RACI. Como parte del proceso de respuesta de incidentes, la RACI debería ser revisada y definida como sea apropiado para el incidente específico. Se debe aprovechar la siguiente tabla como una guía para ayudar a definir la RACI por cada incidente.

Note: As is the case with a list of priorities, RACI charts are subject to change based on the severity and business impact of the incident.

Consultants should provide guidance on how to populate the table below with customer specific details.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Actividad** | **Rol** |  |  |  |  |
|  | **Gestor del incidente** | **Operaciones TI** | **Representante Legal** | **Gestor de Comunicaciones** | **Gerencia** |
| Evaluación inicial | A cargo | Responsable |  |  |  |
| Respuesta inicial | A cargo | Responsable | Consultado | Informado | Consultado |
| Recoger evidencia forense | A cargo | Responsable | Consultado |  | Informado |
| Implementar solución temporal | A cargo | Responsable | Informado | Informado | Consultado |
| Enviar comunicados | Consultado | Consultado | Consultado | Responsable | A cargo |
| Consultar con las autoridades locales | Informado | Informado | Responsable | Informado | A cargo |
| Implementar solución definitiva | A cargo | Responsable | Informado | Informado | Consultado |
| Determinar el impacto financiero | Consultado | Consultado | Consultado | Informado | A cargo  Responsable |

* + 1. Agendamiento

En el caso de un incidente de seguridad alto, la secuencia de actividades de respuesta, podrían ser gobernadas por la severidad y las obligaciones contractuales establecidas por el líder senior, legal, el equipo SIR involucrado en el incidente y las regulaciones de cumplimiento. El equipo SIR, en conjunto con los equipos socios y el gestor de incidentes, establecerán una agenda para ejecutar las actividades de respuesta en consideración con esas obligaciones.

La siguiente línea de tiempo provee un ejemplo a alto nivel de posibles actividades de respuesta e hitos para un incidente de seguridad.

Note: Consultants should work with customers to identify the proper platform and format for communicating status and providing checkpoints. Status updates are critical for problem management and process improvement activities. Checkpoints establish a cadence that Ops teams can use for providing updates. SIR and Executive teams use these checkpoints for managing the incident response and communications activities.

* 1. Comunicar

El equipo SIR entregará actualizaciones periódicas a los principales actores sobre el incidente hasta que éste sea cerrado. La frecuencia de la comunicación y el nivel de detalles deben ser convenidos por adelantado.

* + 1. Comunicaciones Ejecutivas e Informes

Durante la evaluación, la notificación a los líderes ejecutivos es a menudo apropiada y necesaria. Los ejecutivos pueden ayudar en la determinación del impacto total (financiero y de otro tipo) de un incidente de seguridad a toda la organización. Los líderes entregan guía en la respuesta (por ej. quien notifica a los clientes, acciones de relaciones públicas, involucramiento legal temprano, etc.). Finalmente, los líderes proporcionan un vía legítima y rápida a las cadenas de autoridad (por ej. tomar decisiones rápidas para incidentes graves).

* + 1. Declaración de Violación

La declaración de violación involucra comunicar interna y externamente la naturaleza, impacto y respuesta a la violación. La declaración de violación, a menudo se regirá por las leyes de notificación establecidos por los gobiernos. Esas leyes requieren que una entidad que haya sido objeto de una violación de datos, notificar a sus clientes y otras partes acerca de la violación y tomar otros pasos para remediar los daños causados por la violación. Es fundamental estar consciente de los requerimientos y excepciones a esas leyes antes de declarar una violación (por ej. las leyes pueden permitir la notificación tardía en ciertas circunstancias como cuando una agencia de aplicación de la ley determina que la notificación podría impedir una investigación criminal).

Información Adicional:

National Conference of State Legislatures

<http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

US-CERT  
<https://www.us-cert.gov/incident-notification-guidelines#Incident_Notification>

U.S. Department of Health and Human Services

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>

Office of the Australian Information Commissioner

<http://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>

* + 1. Comunicaciones Externas

El equipo de Seguridad y los líderes ejecutivos serán los responsables de entregar la orientación respectiva a todas las comunicaciones con terceros y cual información está siendo diseminada internamente entre organizaciones. Dadas las sensibilidades que rodean este tipo de eventos, ninguna entidad interna o externa debería participar sin la aprobación de los líderes y el equipo SIR.

Sin embargo, se debe estar consciente de que, si la información que se está compartiendo no es precisa o es muy subjetiva, podría ocasionar un daño a la reputación de la organización. Cuando se considere la estrategia de comunicación, se debe considerar buscar apoyo de un experto. Preferiblemente una firma respetable que tenga experiencia in comunicar declaraciones de violaciones, específicamente cuando las comunicaciones están dirigidas a audiencias externas. Aunque pueda existir una necesidad de moverse rápidamente, se debe tener en cuenta que entregar información demasiado pronto, puede significar una violación de datos mayor en la organización. A continuación, se listan puntos a considerar:

* Resistir la comunicación temprana durante el incidente
* Ser cuidadoso en declarar que el incidente está completamente resuelto
* El mensaje inicial debería enfocarse en as medidas tomadas para investigar el incidente

Recuerde, “los hechos” fluidos para entregar declaraciones públicas que pueden resultar en un mal resultado para la empresa, incluyen:

* Difusión inexacta de la información
* Comprometer más datos
* Dañar la reputación de la compañía rompiendo nuevamente la confianza

Considere los siguientes elementos cuando comienza a establecer el mensaje:

* **Los clientes deben ser el foco primario**. La comunicación con ellos debe ser clara y efectiva por medio de canales tradicionales y digitales
* Sin embargo, no se debe olvidar la gran cantidad de actores interesados en violaciones como los reguladores, legisladores y actores de la industria.
* Ser simple, pero integrar los grupos legales, TI, PR y de negocios dentro de la estrategia de comunicaciones
* Pensar en que publicar en los medios sociales
* Los medios entrenan a los ejecutivos
* Configurar los monitores apropiados de plataforma social/de medios y revisar publicaciones
* Desarrollar una estrategia de recuperación de reputación a largo plazo versus tratarlo como un incidente aislado
  + 1. Comunicaciones Internas

Mientras el énfasis a menudo esta puesto en las comunicaciones externas, las comunicaciones internas no deben ser abandonadas. Se debe gastar tiempo determinando cuando informar a los empleados y que informarles. Debido a que esto puede ser incomodo de considerar, la filtración de información ocurre y podría impactar negativamente o alterar dramáticamente el plan de comunicaciones externas. Aun cuando se podría inclinar a informar rápidamente a los usuarios, se debe considerar que todo lo que se informe internamente, estará disponible externamente.

Esto podría hacer pensar que compartir información internamente no es una buena idea. Sin embargo, se pueden tener empleados que trabajan directamente con los clientes y, si se ha compartido información externamente, los clientes les preguntaran a esos empleados o examinaran sus preocupaciones. Independiente de la situación, si existen empleados quienes pueden estar en la situación que un cliente les haga esas preguntas, es necesario considerar que sus respuestas deben haber sido educadas en qué y cómo responder a los clientes. Por ejemplo, si la organización es un banco y se ha descubierto recientemente una violación de seguridad, ¿qué debería decirle un cajeo a los clientes que preguntan o que está visiblemente molesto por el impacto potencial de su información personal? ¿Deberían ser dirigidos al jefe de sucursal? ¿Se tienen tarjetas de información que el cliente puede seguir? Independiente del proceso correcto para la organización, se debe definir el proceso y capacitar a los empleados.

* 1. Responder
     1. Investigar

El siguiente paso crítico en la respuesta a un incidente de seguridad es la investigación. Mientras se investiga un incidente de seguridad, los equipos de SIR y operaciones se enfocarán en un análisis profundo del evento, obtener evidencia forense, determinar la causa raíz y, si es necesario, revisar el alcance original e el impacto del incidente.

Para investigar apropiadamente un incidente de seguridad, debería:

1. Adquirir, organizar y preservar evidencia de una manera que suene forense (desde una perspectiva investigativa versus una de aplicación de la ley), dadas las circunstancias del incidente
2. Iterativamente reevaluar y revisar el ámbito, impacto y severidad del incidente, según más datos sean descubiertos
3. Periódicamente revisar los requerimientos regulatorios de cumplimiento y privacidad
4. Identificar la posible causa raíz del incidente
5. Evaluar, contener, erradicar y las opciones de remediación con los equipos de operaciones para reducir el impacto del incidente
   1. El equipo SIR conducirá la investigación en conjunto con el proceso de gestión de incidentes TI para aprovechar los canales de comunicación existentes, recursos y ritmo de operaciones de cada equipo.
   2. Cada una de las cinco etapas de las fases de investigación son iterativas por naturaleza y pueden ser opcionales dependiendo de múltiples factores como: naturaleza del incidente, disponibilidad/integridad de la evidencia, acceso al medio ambiente, dependencias externas, impacto en los datos principales del cliente, etc.

#### Obtención de Evidencia

Es extremadamente importante identificar, obtener y preservar evidencia perteneciente a un incidente de Seguridad de una forma que no comprometa el proceso forense que está en proceso o uno que es requerido por ley o regulación. Cuando se colecte evidencia, se debe considerar lo siguiente:

* ¿Dónde está la evidencia? Listar que sistemas están involucrados en el incidente y desde cuando la evidencia fue recolectada.
* Establecer que es probable que sea pertinente y admisible. A veces se comete el error de colectar más información de la que es necesaria.
* Por cada sistema, obtener la correspondiente orden de volatilidad.
* Remover vías externas para el cambio.
* Siguiente el orden de volatilidad, colectar la evidencia con las herramientas discutidas en las Sección 5.
* Registrar los tiempos en que se realizan las acciones.
* Preguntarse qué otra cosa en la que trabaja, puede ser evidencia en los pasos de colección.
* Documentar cada paso.
* No olvidar a la gente involucrada. Se debe tomar nota de quién fue y qué fue lo que ellos hicieron, qué observaron y como reaccionaron.
* Cuando sea factible, se debe considerar generar comprobaciones y firmas criptográficas de la evidencia colectada, esto puede hacer fácil preservar una cadena de evidencia fuerte. De esta manera no se alterará la evidencia.

Más evidencia de colección de evidencia y archivado se encontrará acá

<http://www.ietf.org/rfc/rfc3227.txt>

#### Forense

#### Análisis de Causa Raíz (según corresponda)

Según la naturaleza del incidente, los esfuerzos deberían enfocarse en la identificación de la causa raíz del incidente en la medida de lo posible y la validación con los responsables de los servicios. El objetivo principal de llevar a cabo el análisis de la causa raíz es comenzar a determinar el alcance global del incidente e identificar un plan de remediación preliminar para mitigar el impacto. En muchos casos, la identificación de la causa raíz podría no ser posible dentro del plazo de respuesta a incidentes, debido a que la prioridad es la eliminación de posibles vectores de ataques y el foco en los pasos inmediatos para contener el ataque y sus impactos.

#### Revisión del Alcance

La identificación del alcance inicial y ser capaz de revisar el alcance según se descubran más datos en las fases de obtención de evidencia, forense y análisis de causa raíz es esencial para responder adecuadamente a incidentes de seguridad. La revisión del ámbito está enfocada en continuamente evaluar el alcance, impacto y severidad. Esto debería ser un proceso iterativo a lo largo de la investigación y debería descartar posibilidades de impacto cruzado funcional, de servicios y organizacional del incidente de seguridad, el cual significativamente impactará la postura de la respuesta, los esfuerzos de remediación y los requerimientos de notificación.

#### Síntesis de la Investigación

Según la investigación madure desde el diagnóstico inicial a una búsqueda orientada de pruebas, es importante que el equipo de respuesta de incidentes pueda sintetizar los hechos conocidos, líneas de tiempo e impacto descubierto para ser capaz de clasificar el incidente (sección 4.1.2). La siguiente lista entrega una guía para el equipo de incidentes tome una decisión informada para la clasificación del incidente:

Note: Consultants are encouraged to walk thru the checklist with the customer and add/update/remove any artefacts and/or guidance that doesn’t apply.

|  |  |  |
| --- | --- | --- |
| Artefacto | Impacto (NA/Baja/Media/Alta) | Guía |
| Naturaleza del compromiso |  | Tipo de compromiso y el valor de la evaluación involucrada en el compromiso |
| Causa raíz |  | Método de compromiso |
| Método de persistencia |  | Mecanismo que puede facilitar la reentrada en el medio ambiente o para recuperar el acceso a los activos después de la limpieza |
| Duración del compromiso |  | Una línea de tiempo que sugiere un indicador inicial del compromiso y las actividades subsecuentes |
| Actividad maliciosa relevante |  | Cualquier factor circundante que sugieren un posible vínculo al vector identificado del compromiso |
| Pérdida de datos o credenciales |  | Credenciales o datos actuales que se cree que están comprometidos |
| Propietario de activos |  | Departamento TI o unidad de negocios impactada por el compromiso |
| Fuente del ataque |  | Vector de ataque que fue utilizado para iniciar el compromiso |
| Movimiento lateral |  | Activos adicionales accedidos por actores maliciosos después del compromiso inicial |
| Pérdida real |  | Indicación de uso real de los datos o credenciales que se presume que se han robado |
| Víctimas involucradas |  | Sistemas comprometidos usados para el movimiento o salto |
| Atribución del agente |  | Atribución de la intrusión, control o actividad a una persona o grupo |
| Línea de tiempo del agente |  | Registro de tiempo y acciones que podrían ser atribuidas al agente |

Tabla 1: Lista de verificación de investigación

* + 1. Contención

La fase de contención está centrada en la protección de los sistemas de mayor riesgo asociados con el incidente a través de la aislación del sistema. En esta fase, la memoria de los sistemas de interés es probada, los discos son copiados de manera forense y la red es monitoreada.

* Contención y remediación: En el caso de un incidente de Seguridad, el equipo SIR en conjunto con los equipos de operaciones TI y los expertos en la materia desarrollaran una remediación apropiada y un plan de contención para reducir el impacto del incidente de manera oportuna.

Otras consideraciones

* Se debe tratar de evitar que los atacantes sepan que sus actividades fueron descubiertas. Esto puede ser dificultoso, porque algunas respuestas esenciales podrían alertar a los atacantes. Por ejemplo, si hay una sala de emergencia del equipo de SIR o si requiere un cambio inmediato de todas las contraseñas, cualquier atacante interno podría saber que ya se tiene conocimiento del incidente.
* Se debe comparar el costo de apagar los sistemas comprometidos y relacionados contra el riesgo de continuar las operaciones. En la gran mayoría de los casos, se deberían sacar inmediatamente los sistemas de la red. Sin embargo, podrían existir acuerdos de servicio que requieren que los sistemas estén disponibles aun con la posibilidad que ocurra un daño mayor. Bajo esas circunstancias, se puede elegir mantener el sistema en línea con conectividad limitada para poder tomar evidencia adicional durante un ataque.
* En algunos casos, el daño y alcance de un incidente podrían ser tan extensivo que se tendrían que tomar acciones que invoquen una cláusula de penalidad específica en los SLA. En cualquier caso, es muy importante que las acciones que se tomarán en el evento de un incidente sean discutidas previamente y estén descritas en el plan de respuesta para que se pueda tomar una acción inmediatamente cuando ocurra un ataque.
* Se deben determinar los puntos de acceso utilizados por el atacante e implementar medidas para prevenir accesos futuros. Las medidas podrían incluir deshabilitar un modem, agregar entradas de control de acceso a un *router* o *firewall* o incrementar las medidas físicas de seguridad.
* Se debe considerar reconstruir un sistema limpio con nuevos discos duros (los existentes deberían ser removidos y almacenados para que puedan ser usados como evidencia si se decide perseguir legalmente a los atacantes), Se debe asegurar que las contraseñas locales serán cambiadas. También se deberían cambiar las contraseñas de las cuentas de administración y de servicio donde sea que estén en el ambiente.
  + 1. Erradicación

Una parte principal de la recuperación de una intrusión es retomar el control o “recapturar” los sistemas que están bajo control de un atacante. La vía más efectiva de llevar a cabo esto es reconstruir completamente el sistema afectado desde un medio confiable para eliminar cualquier código de un atacante.

NOTA: Antes de reconstruir un host, la organización debería realizar primero un análisis para determinar:

1. Si esto forma parte de operación de envergadura del adversario o si fue un incidente aislado.

2. Si la acción legal puede ser planeada y que información forense debe ser capturada como evidencia.

Mientras que reconstruir el sistema operativo desde un sistema afectado desde una media confiable removerá cualquier código del atacante que exista, los atacantes pueden persistir por otras vías. Estas pueden incluir binarios de la aplicación, datos y estado del usuario como perfiles, así como también a través del robo de credenciales desde el computador. En pocas ocasiones, estas también pueden incluir persistencia por medio de firmware y otros componentes de hardware, pero esto no se ve comúnmente. La reconstrucción del sistema después de un compromiso de seguridad es diferente que una recuperación de desastres porque los atacantes están motivados a persistir en el acceso y se debe tener mucho cuidado para no permitir que los atacantes puedan reintroducirse desde cualquier capa.

Esta sección representa una guía práctica del tipo de actividad requerida para realizar una reconstrucción del host después de un compromiso. Esta guía no debe entenderse como un paso a paso prescriptivo que garantice una remediación exitosa debido a que los atacantes se motivan a adaptarse y persistir.

Reconstruir un Sistema es solo una faceta de la recuperación desde un adversario persistente. Una operación de recuperación debe incluir un enfoque planificado, seguridad operacional, habituación, monitoreo y otras actividades relacionadas.

La siguiente es una lista genérica de “Qué hacer y Qué no hacer” para la reconstrucción de un sistema individual.

HACER:

* Desconectar el sistema desde la red al inicio del evento de remediación y no volver a conectarlo hasta que haya sido resuelto.
* Inventariar todos los programas instalados y datos de la máquina. Se debe asegurar de tener una copia segura de todos los programas, de cualquier configuración de aplicaciones y datos.
* Limpie el disco duro de la máquina para que los datos sean removidos y no se inicie bajo la configuración vulnerable.
* Aun cuando no es absolutamente requerido, es también recomendado que se actualice cualquier ROM/BIOS con la última versión del fabricante.
* Si es posible, utilizar un nuevo nombre para que el antiguo pueda ser monitoreado en caso de reintentos de compromiso.
* Utilizar nuevas contraseñas para cualquier cuenta del sistema. Esto incluye cuentas locales, servicios, trabajos *batch* y cuentas almacenadas dentro de aplicaciones del sistema. También se deberían revisar las cuentas que fueron usadas recientemente en el sistema y que pudieran estar comprometidas.
* Instalar el sistema operativo usando un medio de una fuente de confianza. Revisar el Apéndice C para más detalles.
* Configurar el firewall local o el perfil de la red para bloquear todas las conexiones entrantes hasta que el sistema esté completamente actualizado.
* Aplicar parches y actualizaciones para corregir vulnerabilidades conocidas con el SO.
* Instalar aplicaciones específicas para que puedan realizar su función de negocio previa. Se debe asegurar que se instalen las últimas actualizaciones para eliminar cualquier vulnerabilidad.
* Revisar cualquier configuración de la aplicación restaurada y los datos para scripts, procedimientos u otras personalizaciones que un atacante podría haber dejado para retomar el acceso remoto.
* Cuando sea posible, no restaure ningún perfil de usuario en el sistema y en particular, ponga atención a los datos en puntos de auto ejecución al inicio que pueden ser usados para iniciar aplicaciones cuando el usuario inicia sesión (por ej. registrar la tecla “ejecutar” y el menú de inicio “partida”).
* Inspeccionar los datos restaurados para encontrar cualquier contenido malicioso que pueda ser usado para ejecutar código.
* Cuando sea posible, eliminar cualquier archive .exe y .dll restaurado.
* Buscar virus en todos los contenidos comúnmente explotados, formatos como Microsoft Office, Adobe PFD, HTML, imágenes y videos.
* Conectarse a la red y validar que cualquier política de grupo se haya aplicado.

NO HACER:

* Utilizar programas para reconstruir el sistema que estuvo en la red y podría haber sido manipulado por un atacante.
* Restaurar un respaldo full sobre un nuevo SO porque podría restaurar herramientas del atacante instaladas en la máquina.
* Restaurar datos desde respaldo que usen credenciales comprometidas. Si es necesario, cámbielas antes de permitir el sistema en la red.
* Configurar o actualizar parcialmente el sistema.
  + 1. Recuperación

El retorno de los sistemas a un estado de ejecución segura con operaciones técnicas reportándose como normal, no significa que los servicios se hayan recuperado completamente. Se deben tomar medidas para que los servicios estén completos, en su capacidad normal y disponibles. Esos pasos pueden incluir:

* Las comunicaciones a las partes interesadas indicando que ellos pueden proceder con el uso normal de los sistemas o en algunos casos, restablecer los sistemas por protocoles de seguridad refinados (por ej. requerir cambios de contraseña o aislar la estación de trabajo)
* Los pasos de verificación para asegurar que los servicios hayan sido completamente restaurados para las partes interesadas (por ej. los nuevos permisos implementados para protección previenen el acceso y la consumición de servicios).
* Los procesos de escalamiento y solución del conflicto han sido establecidos en el caso que no se puedan acceder los servicios recuperados como se esperaba o necesitaba.
  1. Cierre
     1. Post mortem

La mejor manera de entender como un incidente de ciberseguridad sucedió es realizando un post mortem. El equipo SIR dirigirá el post mortem del incidente con el equipo de servicio y documentará lo que encuentre y la necesidad de mejoras para mitigar amenazas futuras.

Un post mortem puede incluir lo siguiente:

* Problema – Una descripción del problema y cuando empezó y terminó el incidente.
* Participantes – Quienes participaron activamente en dirigir el incidente. Esto puede ser obtenido desde la matriz RACI.
* Línea de tiempo detallada del incidente (Ver la sección de agendamiento)
  + Marcas de fecha/hora de la actuación y/o acción realizada
  + Acciones realizadas y sus resultados
  + Principales hitos en el plan de recuperación de incidentes (por ej. Notificación Ejecutiva, Erradicación, etc.)
* Causa – ¿Qué acciones o fallas hicieron que este incidente sucediera?
* Manejo
  + ¿Cuáles fueron las medidas tomadas durante el manejo de este incidente?
  + ¿Qué hizo cada participante?
    - Anotar cualquier cosa notoria que un individuo realizó/descubrió (positiva o negativa)
  + Nota: Como fue descubierto finalmente el origen del problema.
* Solución - ¿Cómo se resolvió el problema?
* Prevención - ¿Que se puede hacer para prevenir este incidente y que no vuelva a ocurrir, o minimizar la posibilidad de un re ocurrencia?
* Lecciones aprendidas
  + ¿Qué podría haber hecho mejor en el manejo de este incidente?
  + ¿Qué errores se cometieron en el manejo de este incidente?
  + ¿Qué medidas pueden ser tomados para abordar las deficiencias en el manejo de este incidente?
  + ¿Qué medidas pueden ser tomadas para prevenir los errores que se cometieron o minimizar la posibilidad que vuelvan a ocurrir?
    1. Documentación

Durante un incidente de seguridad, todas las tareas abiertas por los equipos de operaciones deberían ser registradas dentro del sistemas de tickets de [Customer]. El gestor del incidente escogerá el sistema basado en la particularidad del incidente y los equipos de la organización involucrados. Al cierre del incidente, el equipo SIR se asegurará que los tickets relacionados con el incidente se cierren apropiadamente. Todos los detalles colectados durante cada fase de la respuesta del incidente deberían ser capturados e incluidos en una publicación de la revisión de incidente con las propiedades apropiadas.

* + 1. Mejora del Proceso

Una vez que la amenaza haya sido contenida, erradicada y los servicios recuperados, el equipo SIR iniciará el proceso de mejora de actividades que busquen cerrar procesos y/o gaps de rendimiento del sistema. A continuación, algunas preguntas iniciales que pueden ayudar a iniciar el proceso de actividades de mejora:

* ¿Se pudo haber identificado el problema más rápido?
* ¿Se podría haber identificado el incidente de seguridad más pronto?
* ¿Se podría haber detenido el problema tempranamente?
* ¿Qué podría haber ayudado a mejorar la velocidad de esos procesos?
* ¿Se carece de un libro de ejecución? ¿Un proceso? ¿El conocimiento adecuado? ¿Las personas adecuadas en la llamada?
* ¿Se cuenta con los recursos suficientes para manejar estos ataques? ¿Se cuenta con el personal suficiente para monitorear los log del sistema, los log del firewall, los reportes del sistema de detección de intrusos (IDS)?
* ¿Se están utilizando programas para analizar esos log y extraer datos relevantes para minimizar el trabajo de hacerlo manualmente?

1. Apéndice: Lectura Adicional

Respondiendo a los incidentes de Seguridad TI

<https://technet.microsoft.com/en-us/library/cc700825.aspx>

El día después: la primera respuesta a una violación de seguridad

<https://technet.microsoft.com/en-us/magazine/2005.01.incidentresponse.aspx>

Guía de gestión de incidente de seguridad informática

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>