En este capítulo se verán las principales directrices de **cómo gestionar algunos de los incidentes de seguridad más comunes** en una organización.

Hay que mencionar que se asume la existencia de unos protocolos mínimos de actuación que definan los roles del equipo base y del equipo extendido, así como una definición del protocolo de escalada de la información y de su diseminación.

COMPROMISO POR MALWARE

El compromiso por malware es uno de los tipos de incidentes más habituales en una organización. *Equipos zombis que forman parte de una red botnet, infecciones masivas de equipos provocadas por gusanos o ransomware, o equipos comprometidos por RAT (Remote Access Tool) u otro tipo de malware más avanzado* son algunos ejemplos de este tipo de incidentes.

Planificación

Para la detección y la respuesta de este tipo de incidentes es fundamental **contar con elementos técnicos adecuados como antivirus/antimalware, EDR(Endpoint Detection and Response), Host-IDS** o soluciones similares que permitan la protección de los equipos ante el código dañino más habitual y permitan a los analistas monitorizar actividades anómalas en los equipos que pudieran ser un indicativo de compromiso por malware.

Aunque tradicionalmente este tipo de sistemas han basado su funcionamiento en detección basada en firmas o patrones, **son cada vez más las soluciones que incorporan mecanismos más avanzados como detección por heurística, comportamiento, anomalías, incorporación de inteligencia artificial**, etc. lo que las hace más eficaces y se debe tender a ellas puesto que el malware está en continua evolución y cada vez cuenta con unas mayores capacidades de evasión de los sistemas más tradicionales.

Adicionalmente es beneficioso **contar con soluciones** que ayuden a detectar compromisos por malware avanzado, **como herramientas anti APT (Amenaza Persistente Avanzada)** o soluciones que permitan hacer Threat Hunting sobre los medios de la organización.

Estas plataformas deben estar actualizadas y contar con los últimos paquetes de firmas y mecanismos de detección.

Es interesante poder **contar también con soluciones** que permitan **monitorizar el tráfico de red, navegación web del usuario, correos electrónicos, conexiones salientes, volumen de tráfico, carga de CPU de los equipos, etc**.

Detección del incidente y valoración

Este tipo de incidentes suele tener una categoría propia dentro de la taxonomía definida para la clasificación de incidentes de seguridad. En ocasiones, es posible que se hayan definidos subcategorías que perfilen de forma más precisa el tipo de malware al que nos enfrentamos: gusanos, troyanos, ransomware, spyware, adware, etc.

Los compromisos por malware **suelen identificarse principalmente por alertas en los sistemas de monitorización desplegados y por notificaciones de los propios usuarios que reportan situaciones anómalas**. Entre los indicadores de estas amenazas se pueden encontrar *lentitud de los equipos, programas nuevos instalados, ficheros con nombres anómalos o extensiones extrañas presentes en el equipo, complementos nuevos en el navegador, usuarios de dominio bloqueados sin motivo justificable, parada del software antimalware, etc.*

El **ERI** debe identificar lo más fielmente qué tipo de malware es, de cara a plantear estrategias y acciones posteriores en la etapa de respuesta. Para ello es interesante hacerse con una muestra de la pieza de malware detectada y analizarla desde un punto de vista estático y en ocasiones, también desde un punto de vista dinámico o haciendo ingeniería inversa del código. Los objetivos iniciales serían hallar el vector o vectores de entrada del malware, método de propagación si lo hubiere y vulnerabilidades que

aprovecha. De esta forma por ejemplo es posible extraer indicadores de compromiso (hashes, IP o dominios maliciosos, etc.) que permitan ayudarnos a identificar otros equipos afectados, y a una contención rápida de la actividad y de la propagación del código dañino.

En este punto es necesario determinar el alcance de los servicios, dispositivos, o usuarios se han visto afectados por el compromiso o si por ejemplo existe riesgo reputacional, si el incidente afecta a los procesos de negocio de la compañía, a sus operaciones, a nivel de cumplimiento de protección de datos, etc.

Respuesta

Una vez el reporte del incidente haya llegado al **ERI** y éste haya determinado que se trata de un incidente de seguridad se pondrá en marcha el mecanismo de respuesta para contener la infección. **El objetivo es que no se siga propagando el malware y que cese su actividad maliciosa.**

Si el antivirus ha alertado de la amenaza y ha sido capaz de erradicarla esta fase seria sencilla puesto que la amenaza se ha contenido. No obstante, se debe valorar la investigación en muchos casos sobre cómo ha llegado hasta ahí el código dañino. Imaginemos por un momento una alerta del antivirus sobre un código dañino embebido en la descarga de un software pirata que el usuario intenta instalar, en este caso el usuario está incumpliendo la política corporativa poniendo en riesgo a la compañía y, aunque el antivirus haya cumplido con su función bloqueando la amenaza, quizá es necesario tomar algún tipo de medida disciplinaria contra el usuario en cuestión o recordarle que no está permitido el uso de software pirata en la compañía.

Otro caso podría ser la detección de software de hacking avanzado en un equipo como Mimikatz, Metasploit. Cobalt Strike o similares. Este tipo de software tiene una finalidad muy clara y es el compromiso dirigido de los usuarios/equipos. La presencia de este tipo de herramientas en algún equipo, aunque hayan sido bloqueadas, requiere de una investigación para conocer si el usuario está siendo el blanco de algún tipo de ataque.

Si nos enfrentamos al caso de que el malware no ha sido neutralizado por el antivirus debemos identificar las trazas asociadas al software malicioso y analizarlas en profundidad: nuevos ficheros creados en los sistemas infectados, nuevos procesos en ejecución, conexiones anómalas en el Firewall por parte de los equipos víctimas, envío de correos sospechosos desde los equipos investigados, etc.

Una vez el **ERI** ha sido capaz de conocer en profundidad el comportamiento del malware (a través del estudio de las trazas que deja en los equipos afectados, un análisis estático/dinámico, estudios publicados, etc.) debe

aplicar este conocimiento para identificar si existen más equipos afectados y se deben establecer las medidas de contención requeridas, por ejemplo:

- Bloqueo de comunicaciones salientes hacia determinadas IP.
- Filtrado de correos.
- Distribución de actualizaciones.
- Bloqueo desconexión de ciertos puertos/servicios.
- Bloqueo de ciertos usuarios.
- Desconexión de equipos o redes.

Las medidas de contención más drásticas, que impidan el funcionamiento normal de los sistemas deben ser aprobadas convenientemente, siguiendo siempre el procedimiento de gestión de incidentes definido.

En ocasiones es necesario llevar a cabo un análisis forense de los equipos afectados y de los cambios que el malware ha provocado en los mismos, nos

dará información, entre otros, del impacto del incidente al que nos enfrentamos.

La etapa posterior, la erradicación del malware, puede llevarse a cabo a través de las plataformas de antivirus o antimalware con ayuda del fabricante o de forma manual (borrar ciertos archivos, detener determinados servicios, etc.). En caso de no tener una fiabilidad al 100% de que el software malicioso ha sido eliminado se procedería al formateo y reinstalación de los dispositivos afectados.

Se debe tener en cuenta que, en caso de recuperar una copia de seguridad para la restauración de algún sistema, ésta esté completamente limpia y no esté afectada por el compromiso. Además, el malware puede haber obtenido privilegios de administración en las máquinas afectadas así que es preciso hacer un cambio de contraseñas de todos los servicios y usuarios implicados.

Una vez erradicado el malware de la organización, la restauración de los sistemas y vuelta a la normalidad debe hacerse de forma paulatina verificando que los sistemas están completamente desinfectados, no presentan comportamientos anómalos, las contraseñas han sido cambiadas, los equipos han sido reinstalados y tienen todas las medidas de seguridad apropiadas, las copias de seguridad restablecidas están limpias, etc.

Tras ello, los equipos implicados deberán estar sometidos a una vigilancia que confirme que no son reinfectados y que no queda ningún resto de compromiso como una posible puerta trasera en los mismos.

Lecciones aprendidas

Antes de dar por cerrado un incidente de este tipo se debe hacer un análisis retrospectivo identificando las causas de la infección: ¿cómo es posible que el usuario se haya infectado? falta formación concienciación para el usuario?, ¿los mecanismos de detección han funcionado correctamente?, etc.

De igual forma, se debe analizar si la respuesta al incidente ha sido ágil y proporcionada: ¿se pudo haber evitado la propagación masiva del malware de haber actuado antes?, se detectó el incidente a través de la plataforma de monitorización o a través de un reporte por parte de un usuario o un tercero?, ¿cómo mejoramos la detección por parte de la plataforma de monitorización? ¿hemos sido capaces de erradicar el malware de forma automática? ;disponemos de herramientas adecuadas para hacer una contención ágil de los equipos o redes afectadas? ¿hemos sido capaces de aislar todos los equipos afectados? ¿se ha respondido con proporcionalidad

o podríamos haber aplicado medidas que no impidiesen la operativa normal del empleado?, etc.

Analizadas todas las cuestiones se cerraría el informe final del incidente planificándose, si quedan por abordar, todas aquellas propuestas de mejora o cambios a realizar para que el incidente no vuelva a repetirse y de hacerlo seamos capaces de reaccionar de forma más eficaz.

CASO ESPECIAL MALWARE: RANSOMWARE OPERADO

Puesto que los incidentes por ransomware son de gran interés por el impacto que causan, se ha decidido añadir un caso de estudio especial.

Para ponernos en antecedentes, se expondrá como suelen tener lugar este tipo de compromisos, esto es el ciclo de vida de esta amenaza. En primer lugar, en cuanto a la fase de acceso inicial, actualmente los ataques de ransomware más comunes se basan en campañas de correo fraudulento, bien de tipo spear-phishing, bien campañas de phishing a múltiples usuarios de la organización.

Otros vectores de ataque que se han detectado en este tipo de ataques es la explotación de vulnerabilidades, sobre todo en sistemas expuestos a Internet, a través de cuentas de usuarios comprometidas que tuviesen privilegios para hacer el despliegue del ransomware, o a través de dispositivos externos como

USB que puedan permitir la ejecución y propagación de un malware de esta índole por la red corporativa.

Posteriormente, en la fase de ejecución, los correos que reciben las víctimas contienen un documento adjunto (o una URL que lo descarga) con diferentes extensiones como .pdf, .doc, .xls, etc. e instrucciones de como ejecutarlo. Una vez recibido el correo en la bandeja, si la víctima descarga el archivo malicioso y lo ejecuta en su equipo, se produce la infección. dando lugar a las primeras fases de la infección.

A continuación, el atacante comienza a obtener credenciales mediante herramientas como Mimikatz y a realizar movimientos laterales con otras herramientas de postexplotación como PowerShell Empire o Cobalt Strike.

Tras la obtención por parte del atacante de credenciales de diferentes cuentas de usuario suele consigue escalar privilegios y establecer conexión con los servidores de Comando y Control, procediendo a continuación a cifrar los

sistemas corporativos mediante, haciendo uso de herramientas como PsExec o GPO y usando diferentes familias de ransomware.

En función de la criticidad de los sistemas cifrados y la información que estos contienen, variará el Impacto que el atacante logra obtener.

Finalmente, cuando los atacantes han conseguido cifrar los sistemas de la organización comienzan a extorsionar a la misma solicitando dinero a cambio de descifrarles la información. En ataques recientes de este tipo, los atacantes previamente al cifrado de la información han realizado una exfiltración de la misma con lo que también amenazan a las compañías con revelar esta información en caso de no pagar el rescate.

Planificación

En esta etapa, se deben considerar varios aspectos de bastionado fundamentales, tales como:

- Auditoría y control de visibilidad sobre qué servicios de la compañía están expuestos en internet.
- Verificación de que tanto el Firewall como el sistema antispam están debidamente configurados.
- Control del uso de protocolos con vulnerabilidades como LM/NTLM.
- Bastionado y auditoria del Directorio Activo
- Concienciación de los usuarios. Explicar por ejemplo el impacto que puede ocasionar abrir un archivo procedente de un correo sospechoso. Qué hacer en caso de recibir correos maliciosos, como se deben notificar al equipo de seguridad, etc.

Es importante educar a los usuarios sobre las distintas técnicas de ingeniería social que más utilizan los atacantes para obtener información relevante (llamadas telefónicas fraudulentas, SMS extraños, etc.).
Conviene hacer ciberejercicios para evaluar el nivel de conocimiento de los usuarios.

- Control de la ejecución de PowerShell.
- Segmentación adecuada de las redes de la organización que ayude a reducir el alcance de una posible infección. Revisión de VLAN, máquinas de salto, ACL, NAC, etc.
  Es conveniente disponer de una segmentación de red adecuada en la que se incluya un equipo concentrador de salto al que los administradores de sistemas accedan y de ahí a los equipos a administrar. El equipo concentrador de salto debe estar bastionado con reglas muy críticas y deben estar muy claras las políticas a seguir para determinar quién accede a qué equipos desde ese concentrador de salto. Políticas aún más

restrictivas serían el uso de Paw (Privileged Access Workstations), que son puestos bastionados que solo se usen para administrar los sistemas o el establecimiento de que a los servidores solo se pueda acceder a través de máquinas de salto.

- Control de permisos de los usuarios. Se recomienda restringir el número de cuentas con privilegios
- Configuración segura del correo electrónico a través del uso de herramientas de sandboxing, políticas antimalware y antiphishing, con una política restrictiva sobre los adjuntos que se admiten, etc.
- Control del nivel de parcheado del parque de equipos de la organización.
- Hacer uso de doble factor de autenticación para los accesos a la red de la organización.
- Restringir el uso de habilitación de macros en los documentos Office.
- Despliegue de LAPS herramienta que proporciona administración de contraseñas de cuentas locales de equipos unidos al dominio.

- Disponer de copias de seguridad de la información que no se deba perder.
- Disponer de un Plan de Recuperación ante Desastres (DRP, Disaster Recovery Plan) y un Análisis de Impacto del Negocio (BIA, Business Impact Analysis).

Desde el punto de vista de fuentes a monitorizar es importante tener visibilidad sobre toda la tecnología implicada en los puntos enumerados anteriormente: alertas que provengan de la plataforma antiphishing antispam, control de los accesos remotos, detección a nivel de endpoint de procesos sospechosos, detección de usos anómalos de herramientas de control remoto, monitorización del uso de PowerShell, etc.

Por supuesto es fundamental contar con procedimientos para la gestión de este tipo de incidentes, realizar simulacros periódicos y mantener toda la documentación implicada actualizada.

Conociendo en detalle el modus operandi de cada tipo de ransomware se pueden crear reglas de correlación específicas como, por ejemplo:

- Campaña de correos phishing detectada.
- Accesos a URL sospechosas.
- Múltiples alertas del Firewall para un mismo equipo.
- Instalación de un nuevo servicio en un equipo.
- Detección de Cobalt Strike en un equipo.
- Múltiples equipos con el mismo fichero malicioso.
- Posible robo de credenciales.
- Acceso por fuerza bruta a servidores críticos.
- Modificación del grupo Administradores del dominio.
- Accesos de un usuario Administrador fuera del horario de oficina.
- Exfiltración de datos por SMB.

Detección del incidente y valoración

Una vez se ha detectado el compromiso, las acciones posteriores deben centrarse en obtener la máxima información sobre la amenaza, ya que este conocimiento nos ayudará a definir las acciones de respuesta, tanto de contención como de erradicación de la misma. Es por tanto preciso:

- Determinar qué tipo de ransomware ha infectado a la compañía. Si es conocido o no, si es posible descifrar la información (si hubiese sido cifrada), cómo se propaga etc.
  - Extraer indicadores de compromiso (ficheros, hashes, procesos, conexiones de red, etc.).
- Determinar el alcance de la infección identificando a qué y cómo ha afectado el ransomware a la organización y a su negocio.
  - Realizar una búsqueda de los indicadores de compromiso en la red corporativa, para ello se puede hacer uso de herramientas antivirus, EDR, registros de los sistemas, etc.

  - Identificar a qué tipo de datos ha afectado el ransomware.
- Evaluar el impacto analizando la criticidad de la información que se ha visto comprometida, servicios paralizados, pérdidas económicas, etc.
  - Si ha habido fuga de información como sucede en muchos episodios de incidentes por ransomware en los que el atacante no solo cifra la información, sino que amenaza con publicarla si no se paga el rescate) se debe evaluar de la forma más conveniente la gestión del incidente. En el siguiente punto se explica un ejemplo de incidente por fuga de información.
- Intentar identificar el vector de entrada.

Es necesario recordar que existe cierta obligatoriedad de notificación de algunos incidentes ante determinados organismos, como hemos visto en capítulos anteriores. En este punto se debe plantear una comunicación con estos organismos. No hay que olvidar tampoco que es obligatorio poner en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado este tipo de

incidentes ya que el silencio solo hace que contribuir al aumento de estos delitos.

Respuesta

La etapa de respuesta tiene como objetivo identificar qué acciones debe llevar a cabo la organización tras haber sido detectado el incidente por ransomware para contener el ataque y reducir el impacto que este pueda tener. Ejemplos de algunas de estas acciones podrían ser:

- Aislar los equipos infectados creando redes de cuarentena.
- Analizar todos los equipos en busca de identificar cuales están infectados.
- Filtrar en el perímetro las direcciones IP y dominios maliciosos identificados.
- Eliminar o detener los procesos maliciosos identificados que puedan tener relación con el ransomware.
- Deshabilitar las cuentas de usuario comprometidas.
- Cambiar credenciales de todos los usuarios, sistemas y aplicaciones corporativas que estuvieran dentro del alcance del compromiso.

- Eliminar de las bandejas de entrada de los usuarios todos aquellos correos que pudieran tener relación con el ataque.
- Tomar las medidas necesarias en la plataforma de correo para evitar la nueva entrada de los correos maliciosos identificados.

Tras la contención y la erradicación de la amenaza se debe proceder a la restauración de los servicios afectados de la organización. Para ello, algunas acciones que se deberían llevar a cabo son las siguientes:

- Plantear la creación de una nueva red limpia diseñada de cero y bastionada para ir incorporando los sistemas restaurados (tal y como se ha explicado con anterioridad cuando hablábamos del modelo de red limpia, red gris y red sucia).
- Restaurar copias de seguridad previamente analizadas y descartando posibles indicios de infección en las mismas.

- Restaurar equipos cumpliendo con la política de seguridad de los puestos de usuarios de la compañía.
- Revisar que todos los equipos y servidores están parcheados y bastionados.
- Vigilar los equipos restaurados con especial interés en busca de posibles reinfecciones.
- Es conveniente que la organización disponga de un plan de Recuperación ante Desastres y un Análisis de Impacto del Negocio que, entre otros aspectos, en caso de recuperación de entornos completos indique el orden de la secuencia de arranque de los equipos y la prioridad de los mismos.

Hasta aquí, todas las acciones mencionadas eran eminentemente técnicas u operativas, pero no hay que olvidar la gestión del incidente desde el punto de vista estratégico y responder a preguntas como:

- ¿Qué directrices de comunicación interna se siguen? ¿Y externa?
- ¿Hay responsabilidades legales? ¿Qué medidas se tomarán al respecto?
- ¿Es necesario pedir ayuda externa? ¿Cómo se contrata?
- ¿Cómo nos comunicamos si nuestros canales de comunicación se han visto inhabilitados por el incidente? ¿Se dispone de un plan alternativo?
- ¿Almacenamos los datos cifrados que no se han podido recuperar por si en el futuro se obtiene la clave de descifrado?
- ¿Se ha publicado información sobre el incidente en los medios de comunicación? ¿Cómo se procede?

Lecciones aprendidas

Se debe analizar la gestión realizada del incidente intentado esclarecer aspectos tales como si se hubiese podido detectar antes el compromiso, si es necesario establecer medidas de protección y detección o mejorar las ya existentes, valorar si la recuperación de la información ha sido la adecuada, etc. Otras preguntas que se deben responder podrían ser las siguientes:

- ¿Se disponían de copias de seguridad?, ¿la restauración de las copias de seguridad ha sido ágil?
- ¿Qué RTO (Recovery Time Objetive o Tiempo Objetivo de Recuperación) y RPO (Recovery Point Objetive o Punto Objetivo de Recuperación) existen?
  - El RTO es el tiempo definido dentro del nivel de servicio en el que un proceso de negocio debe ser recuperado después de un desastre o pérdida para así evitar consecuencias debido a la ruptura de continuidad de servicio.

- El RPO es la medición de la cantidad máxima de información que se puede perder. Ayuda a medir cuanto tiempo puede pasar entre la última copia de seguridad y el desastre sin causar demasiado daño al negocio.

- En caso de ser necesario ¿se disponía de stock de hardware para emergencias como la sufrida?
- ¿La comunicación entre departamentos ha sido fluida? ¿Existía una estrategia de comunicación definida hacia terceros? ¿Ha sido la adecuada? ¿Se ha comunicado entiempo y forma a todos los implicados?
- ¿Se ha filtrado información sobre el incidente? ¿Por parte de quién? ¿Se tomarán medidas al respecto? ¿Cómo evitar que esto vuelva a ocurrir?

FUGA DE INFORMACIÓN

La fuga de datos implica, principalmente si afecta a información sensible, un alto impacto para cualquier compañía, incluyendo ámbitos como el reputacional o el legal. Los equipos de respuesta ante incidentes deben estar especialmente preparados ante este tipo de incidentes ya que su impacto puede ser muy alto.

Planificación

Uno de los mecanismos principales para mitigar los riesgos asociados a las fugas de información pasa por establecer en la organización una política de seguridad dentro de la cual se especifique el procedimiento de clasificación y tratamiento de la información acorde a los requisitos de seguridad corporativos. Dicho procedimiento debe especificar detalladamente al menos los siguientes aspectos:

- Clasificación de la información.

- Restricciones de tratamiento, incluyendo etiquetado, almacenamiento, transmisión, copia y difusión.
- Marcado de soportes físicos, si aplica.
- Tiempos de vida y caducidad de la información.
- Protocolo de destrucción de la información.

Todo el personal de la organización debe conocer las directivas de clasificación y tratamiento de la información corporativa y cumplir y hacer cumplir las mismas, notificando al Departamento de Seguridad cualquier posible desviación observada al respecto.

Deben establecerse los acuerdos de confidencialidad correspondientes en cada caso (NDA, Non Disclosure Agreement) y éstos deben ser aceptados mediante firma por todo el personal con acceso a información relevante, tanto externo como interno a la organización, con sus correspondientes procedimientos disciplinarios en caso de incumplimiento. De forma adicional,

en el caso de información clasificada, deben establecerse las habilitaciones y restricciones correspondientes en función del tipo de información tratada.

Además, la organización debe analizar la conveniencia de implantar y operar al menos los siguientes elementos de monitorización y control con el fin de detectar o evitar fugas de información:

- Sistemas DLP
- Sistemas de monitorización de fuentes externas.
- Mecanismos de identificación de insiders.
- Bastionado mínimo de los sistemas que custodian la información.

Detección del incidente y valoración

Es fundamental actuar con la máxima celeridad cuando se detecta que podemos estar ante una posible fuga de información. A mayor rapidez de contención del incidente menor impacto ocasionará el mismo. De confirmarse la fuga de información, el equipo de respuesta ante incidentes de determinar al menos los siguientes aspectos:

- Tipo de información exfiltrada.
- Cantidad de información fugada.
- Origen de la fuga y posibles causas de ésta.
- Potenciadores del impacto, identificando que elementos incrementan el daño causado por la fuga: difusión pública, intereses económicos o políticos, etc.
- Identificar quién o quiénes han recibido la información extraída y que uso podrían hacer de ella.

- Estrategia de comunicación, en caso de ser necesario.

El analista probablemente detectará la fuga de información por una alerta en sus sistemas de monitorización (accesos indebidos, casos de uso sobre exfiltración de la información, etc.), por posible extorsión por parte de un tercero o por la publicación de la información sustraída en un medido externo a la organización.

Respuesta

Los mecanismos de respuesta comenzarán con las acciones relacionadas con la contención del incidente como, por ejemplo:

- Acciones destinadas a cerrar la fuga de datos producida y a evitar nuevas fugas relacionadas. Este tipo de acciones son prioritarias para evitar un impacto mayor.
- Acciones destinadas a minimizar la difusión de la información.
- Acciones destinadas a proteger a los actores potencialmente afectados por la fuga de información (personas, sistemas, etc.).
- Acciones de identificación de las consecuencias de la fuga (legales, económicas, reputacionales) e iniciativas para minimizar el impacto.
- Acciones que impliquen relaciones con terceros (FFCCSE, CSIRT de referencia, medios de comunicación, etc.).

Para la etapa de erradicación del incidente se deben tener en cuenta:

- Acciones que soluciones las vulnerabilidades técnicas identificadas por las que se ha producido la fuga de información.
- Si la causa de la fuga ha sido humana, se deberán tomar las medidas pertinentes. Si ha sido por ejemplo por un fallo en las políticas de seguridad corporativa éstas deberán ser modificadas. Si ha habido intencionalidad se deberá ampliar la investigación al entorno de actuación del insider.
- Si los datos han sido publicados en sitios públicos se deberá contactar con los responsables de estos sitios para que se elimine la información publicada.

Tras las etapas anteriores la etapa de recuperación pasaría por la restauración de todos los elementos involucrados en el incidente a su estado original considerado seguro. En ocasiones será necesario la reinstalación completa de sistemas, un bastionado adecuado, restauración de copias de seguridad, despliegue de nuevos controles de prevención de fugas de información, etc.

Lecciones aprendidas

Ante una fuga de información, la organización debe evaluar la eficiencia de los controles de seguridad definidos, tanto en el plano técnico como en el plano organizativo, con la finalidad de determinar si son adecuados y en qué medida se podrían reforzar.

El equipo de respuesta ante incidentes debe valorar si ha actuado con diligencia en todas sus acciones y si las comunicaciones con los afectados y otros terceros han sido las adecuadas. Otro tipo de preguntas que se deberían responder son las siguientes: ¿la información estaba suficientemente protegida? ¿se puede poner algún mecanismo técnico que evite la fuga de la información? ¿se puede concienciar mejor a los usuarios sobre el uso de la información interna de la compañía?, etc.

INTRUSIONES

Las intrusiones en sistemas de información son otro de los incidentes a los que un equipo de respuesta ante incidentes deberá enfrentarse en algún momento. Un intruso que haya conseguido el nivel de privilegio adecuado en los sistemas corporativos puede desencadenar incidentes de muy alta criticidad en la organización, no sólo por la intrusión en sí misma sino por efectos colaterales a partir de ésta: fugas de información, instalación de malware, alteración de la información, eliminación de datos, etc.

Por este motivo, como en la gestión de cualquier incidente, las capacidades para detectar y responder adecuadamente en el menor tiempo posible son clave para que el impacto asociado al incidente sea lo más pequeño posible.

Planificación

En este tipo de incidentes, como en cualquier otro, se deben plantear las consideraciones habituales de esta fase como la concienciación y formación de los usuarios, la elaboración de procedimientos operativos probados y validados, implantación de controles técnicos adecuados y especialmente un despliegue y operación de un sistema completo de monitorización, capaz de identificar situaciones anómalas significativas de una intrusión. Es conveniente evaluar el uso de sistemas NIDS, HIDS, un sistema SIEM o equivalente que centralice logs, herramientas anti-APT, sistemas de contrainteligencia, etc. y diseñar los casos de uso apropiados para explotar todos los datos ofrecidos por todas estas fuentes con eficacia.

Detección del incidente y valoración

El equipo de gestión de incidentes deberá recopilar inicialmente toda la información disponible relativa al incidente, como podría ser:

- Trazas de red a través del NIDS.
- Actividad en los sistemas comprometidos (procesos sospechosos, ficheros accedidos).

Se deberán abordar preguntas como ¿cuál ha sido el origen de la intrusión? ¿cuándo se ha producido la intrusión y cuando ha sido detectada? ¿cuáles son los sistemas, usuarios o datos comprometidos? ¿qué acciones ha podido hacer o ha hecho el intruso?, etc.

Respuesta

En esta etapa la primera acción de contención que deberá realizar el equipo de gestión de incidentes es el de hacer una copia de seguridad del estado actual del entorno comprometido, en especial de las evidencias volátiles, para un análisis posterior si así se requiere. Una vez salvaguardadas las evidencias del entorno comprometido se procederá a aislar los sistemas afectados.

Se deben analizar no solo los sistemas de los que se tiene constancia que han estado vulnerados sino también aquellos a los que el atacante haya podido tener acceso potencial.

El análisis realizado sobre los equipos deberá proporcionar información de interés para el equipo de analistas de cara a llevar a cabo la erradicación de la amenaza, así como determinar el alcance de la intrusion (fallos o vulnerabilidades en aplicaciones o sistemas, configuraciones incorrectas,

etc.). En algunos casos será necesario un análisis forense en profundidad de los sistemas afectados.

Siempre que sea posible, la recomendación para la recuperación ante un incidente de estas características es instalar de cero un nuevo entorno y sobre el restaurar la última copia de seguridad disponible y que ofrezca un nivel de confianza aceptable, descartando que dicha copia también pudiera estar comprometida.

Lecciones aprendidas

Será necesario evaluar que debilidades técnicas u organizativas han sido aprovechadas por el atacante para llevar a cabo la intrusión y establecer mecanismos de seguridad para mejorar los controles correspondientes.

El equipo de respuesta ante incidentes deberá responder a preguntas como ¿se disponen de herramientas para monitorización de movimientos laterales? ¿se disponen de casos de uso específicos para detectar intrusos? ¿se puede mejorar la seguridad de la gestión de los accesos?

ATAQUE DE DENEGACIÓN DE SERVICIO

De acuerdo a la guía CCN-STIC-817 [10] un ataque de tipo "Disponibilidad" se define como: "Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas."

Una denegación de servicio puede ser ejecutada a través de múltiples técnicas; la más habitual corresponde a inundaciones o saturación de dispositivos por tráfico o peticiones. Otras posibles técnicas pueden incluir el aprovechamiento de vulnerabilidades o errores de configuración.

Planificación

Además de los controles habituales de seguridad y procedimientos de gestión de incidentes sería conveniente disponer de una serie de salvaguardas previas para la mitigación de ataques de tipo DoS/DDoS:

- Servicio antiDDoS del proveedor de acceso a Internet con soporte y servicio de alerta temprana.
- Sistemas de seguridad perimetrales correctamente configurados (Firewalls, IPS, balanceadores de tráfico, etc.).
- Monitorización en fuentes públicas o privadas en busca de potenciales amenazas o indicios de campañas de ataques de denegación de servicio contra la infraestructura.
- Disponer de un dispositivo de gestión de ancho de banda en el perímetro.

Sería también interesante establecer mecanismos de actuación conjunta tanto para la detección como para la respuesta con los departamentos de sistemas y comunicaciones

Detección del incidente y valoración

Habitualmente un incidente DDoS puede ser identificado a través de los siguientes mecanismos:

- Notificación de usuarios o terceros.
- Servicio AntiDDoS del proveedor de comunicaciones.
- Equipo de Comunicaciones/sistemas perimetrales
- Monitorización activa en fuentes abiertas.
- Otros.

El equipo de analistas deberá responder en esta etapa a preguntas como: ¿qué servicios están afectados y en qué grado?¿desde cuándo? ¿qué flujo de tráfico está causando el incidente? (identificar IP origen, IP destino, protocolo, tipo de petición, etc.), ¿el departamento de comunicaciones tiene información que nos pueda ayudar a la investigación? ¿el servicio antiDDoS

del proveedor de Internet nos ha notificado y tienen información de interés? ¿disponemos de trazas de ciberataques o tráficos anómalos externos?

Respuesta

Ante un ataque de estas características es importante que la información interdepartamental fluya de forma ágil y tanto la dirección como las áreas técnicas estén enteradas en todo momento del estado del incidente. Es conveniente también ante una pérdida total o parcial de servicios se alerte al equipo de Service Desk o Centro de Atención al Usuario sobre lo que está sucediendo -sin dar información sensible, para que puedan atender oportunamente el aluvión de llamadas de los usuarios que puedan tener.

La etapa de contención en este tipo de incidentes es compleja y habitualmente se requiere del servicio antiDDoS contratado. Algunas de las acciones que se llevarían a cabo son las siguientes:

- Confirmar con el servicio AntiDDoS la aplicación de las medidas de filtrado por defecto sobre los direccionamientos afectados. En caso de detectar tráfico específico no publicado, solicitar su bloqueo directamente.

- Solicitar al servicio AntiDDoS la aplicación de las medidas de filtrado por geolocalización sobre la dirección IP afectada.
- Bloquear en perímetro:
  - Acceso desde las direcciones IP originadoras del ataque o de listas negras de mala reputación
  - Tráficos dañinos si se ha sido capaz de identificarlos (protocolos, cabeceras, etc.), siempre que no afecten al servicio legitimo.
  - Acceso total a las direcciones IP afectadas por el ataque en caso que estas correspondan a servicios secundarios.

Tras contener el ataque se deberá pasar a la etapa de erradicación del mismo con acciones como:

- Aplicación de actualizaciones necesarias en caso de que la denegación de servicio hubiese sido provocada por el aprovechamiento de una vulnerabilidad.

- Evaluar una restructuración de los elementos de red en el perímetro.
- Evaluar la aplicación de nuevos filtros de seguridad en los elementos perimetrales.

Las medidas aplicadas para la contención serán deshabilitadas si así se requieren, pero siempre de forma progresiva antes de volver a la situación de normalidad.

Recordar que es importante el registro del incidente con información precisa principalmente sobre:

- Hora inicio del ataque.
- Método de detección.
- Objetivo del ataque.
- Inicio de la mitigación.
- Tipo de ataque.
- Hora de la restauración del servicio.

- Hora de fin del ataque.
- Cualquier otra información relevante.

Lecciones aprendidas

Es preciso valorar si han tomado o se deben tomar medidas extraordinarias para mitigar el impacto de este tipo de ataques:

- Verificar el funcionamiento del servicio antiDDoS contratado.
- Si se ataca una página Web valorar disponer de una copia estática de la misma.
- En el caso de los servidores Web, por ejemplo:
  - ¿Se dispone de un WAF?
  - ¿Se limita el número de conexiones máximas simultáneas?
  - ¿Se controla el número de conexiones desde una única IP?
  - ¿Se hace uso de captcha para la autenticación?
- Revisar las configuraciones de los dispositivos perimetrales, entre otros:
  - Bloquear conexiones con User-Agent relacionados con herramientas de hacking.

- Bloquear tráfico proveniente de la red TOR.
- Activar el módulo de IPS.
- Activar la protección contra SYN Flood.

De igual forma hay que valorar si el plan de continuidad de negocio contempla un ataque de este tipo y si su puesta en marcha ha funcionado para minimizar el impacto del ataque sobre el negocio.

- *Capítulo del libro Gestión de incidentes de ciberseguridad. Autor: María Teresa Moreno García. Editorial RA-MA*