Capítulo 7
Operaciones de seguridad

Este capítulo trata los siguientes temas:

- **Investigaciones:** Los conceptos discutidos incluyen investigaciones y procedimientos forenses y digitales, informes y documentación, técnicas de investigación, recolección y manejo de evidencias, y herramientas, tácticas y procedimientos forenses digitales.

- **Tipos de investigación:** Los conceptos discutidos incluyen operaciones/administrativas, penales, civiles, regulatorias, normas de la industria e investigaciones de exhibición de documentos electrónicos.

- **Actividades de registro y monitoreo:** Los conceptos discutidos incluyen auditoría y revisión, detección y prevención de intrusiones, información de seguridad y gestión de eventos, monitoreo continuo y monitoreo de egresos.

- **Aprovisionamiento de recursos:** Los conceptos discutidos incluyen inventario y administración de activos, administración de configuraciones, activos físicos, activos virtuales, activos en la nube y aplicaciones.

- **Conceptos de operaciones de seguridad:** Los conceptos discutidos incluyen la necesidad de conocer/menos privilegios; administrar cuentas, grupos y roles; separación de funciones y responsabilidades; gestión de cuentas con privilegios; rotación de puestos de trabajo y vacaciones obligatorias; control de dos personas; procedimientos de información confidencial; retención de registros; ciclo de vida de la información; y acuerdos de nivel de servicio.

- **Protección de recursos:** Los conceptos discutidos incluyen la protección de activos tangibles e intangibles y la gestión de medios, hardware y activos de software.

- **Gestión de incidentes:** Los conceptos discutidos incluyen eventos contra incidentes, investigaciones de incidentes y equipos de respuesta a

incidentes, reglas de participación, autorización, alcance, procedimientos de respuesta a incidentes, administración de respuesta a incidentes y los pasos en el proceso de respuesta a incidentes.

- **Medidas de detective y preventivas:** Los conceptos discutidos incluyen IDS/IPS, firewalls, lista blanca/lista negra, servicios de seguridad de terceros, espacio aislado, honeypots/honeynets, anti-malware/antivirus, niveles de recorte, desviaciones de estándares, eventos inusuales o inexplicables, reinicios no programados, divulgación no autorizada, recuperación de confianza, rutas de confianza, controles de entrada/salida, endurecimiento del sistema y sistemas de administración de vulnerabilidades.

- **Gestión de parches y vulnerabilidades:** Los conceptos discutidos incluyen el proceso de administración de revisiones empresariales.

- **Procesos de gestión de cambios:** Los conceptos discutidos incluyen los procesos de administración de cambios.

- **Estrategias de recuperación:** Los conceptos discutidos incluyen la creación de estrategias de recuperación; estrategias de almacenamiento de copia de seguridad; recuperación y múltiples estrategias de sitio; sistemas, instalaciones y energía redundantes; tecnologías de tolerancia a fallos; seguro; copia de seguridad de datos; detección y extinción de incendios; alta disponibilidad; calidad del servicio; y la resiliencia del sistema.

- **Recuperación ante desastres:** Los conceptos discutidos incluyen respuesta, personal, comunicaciones, evaluación, restauración y capacitación y sensibilización.

- **Pruebas de planes de recuperación ante desastres:** Los conceptos discutidos incluyen prueba de lectura, prueba de lista de verificación, ejercicio de mesa, prueba estructurada, prueba de simulación, prueba paralela, prueba de interrupción completa, taladro funcional y taladro de evacuación.

- **Planificación y ejercicios de continuidad del negocio:** Los conceptos discutidos incluyen la planificación y los ejercicios de continuidad del negocio.

- **Seguridad física:** Los conceptos discutidos incluyen controles de seguridad perimetrales y controles de seguridad internos.

- **Seguridad del personal:** Los conceptos discutidos incluyen coacción, viajes, monitoreo, manejo de emergencias y capacitación y conciencia de seguridad.

Las operaciones de seguridad incluyen conceptos de operaciones de seguridad fundamentales, investigaciones, administración de incidentes y recuperación ante desastres. También cubre la seguridad física y del personal. Los

profesionales de la seguridad deben recibir la formación adecuada en estas áreas o emplear expertos en estas áreas para garantizar que los activos de la organización estén debidamente protegidos.

El dominio Operaciones de seguridad aborda una amplia gama de temas, incluidos investigaciones, registro, supervisión, aprovisionamiento, conceptos de operaciones de seguridad, protección de recursos, administración de incidentes, medidas de detectives y preventivos, administración de parches y vulnerabilidades, administración de cambios, recuperación ante desastres, continuidad del negocio, seguridad física y seguridad del personal. Del 100% del examen, este dominio tiene un peso medio del 13%, que es el tercer peso más alto de los ocho dominios y está vinculado con otros dos dominios. Por lo tanto, prestar mucha atención a los muchos detalles en este capítulo!

Las operaciones de seguridad implican garantizar que todas las operaciones dentro de una organización se lleven a cabo de forma segura. Se refiere a investigar, gestionar y prevenir eventos o incidentes. También abarca las actividades de registro a medida que se producen, el aprovisionamiento y la protección de recursos según sea necesario, la administración de eventos e incidentes, la recuperación de eventos y desastres y la seguridad física. Las operaciones de seguridad implican el funcionamiento diario de una organización.

TEMAS DE LA FUNDACIÓN

INVESTIGACIONES

Las investigaciones deben llevarse a cabo de la manera adecuada para garantizar que cualquier prueba recopilada pueda ser utilizada en los tribunales. Sin las investigaciones adecuadas y la recolección de pruebas, los atacantes no serán considerados responsables de sus acciones. En esta sección discutimos investigaciones y pruebas forenses y digitales.

Investigaciones forenses y digitales

Las investigaciones informáticas requieren procedimientos diferentes a los de las investigaciones regulares porque el plazo para el investigador está comprimido y un experto podría ser requerido para ayudar en la investigación. Además, la información informática es intangible y a menudo requiere un cuidado adicional para garantizar que los datos se conserven en su formato original. Por último, las pruebas de un delito informático son mucho más difíciles de reunir.

Una vez que se haya tomado la decisión de investigar un delito informático, debe seguir los procedimientos estandarizados, incluidos los siguientes:

- Identificar qué tipo de sistema se va a incautar.
- Identifique a los miembros del equipo de búsqueda e incautación.

- Determine el riesgo de que el sospechoso destruya pruebas.

Después de que las fuerzas del orden han sido informadas de un delito informático, las limitaciones del investigador de la organización se incrementan. Entregar la investigación a las fuerzas del orden para garantizar que las pruebas se conserven adecuadamente podría ser necesaria.

Al investigar un delito informático, deben abordarse las normas probatorias. Las pruebas informáticas deben probar un hecho que es material para el caso y debe ser confiable. La cadena de custodia debe mantenerse, como se describe más adelante en el capítulo. Es menos probable que las pruebas informáticas sean admitidas en los tribunales como prueba si el proceso para producirla no ha sido documentado.

> **nota**
>
> Si bien la mayoría de la discusión de las investigaciones se centra en investigaciones criminales, las organizaciones también deben considerar investigar las acciones del personal que pueden violar las políticas corporativas. Por ejemplo, es posible que las organizaciones quieran supervisar al personal para asegurarse de que no se está infringido la directiva de uso aceptable (AUP). Los profesionales de la seguridad deben asegurarse de que estas investigaciones se coordinen para incluir personal de recursos humanos. Las investigaciones internas a menudo pueden ser tan importantes como las investigaciones criminales.

Cualquier investigación forense implica los siguientes pasos:

1. identificación
2. preservación
3. colección
4. examen
5. análisis
6. presentación
7. decisión

El proceso de investigación forense se muestra en la Figura 7-1.

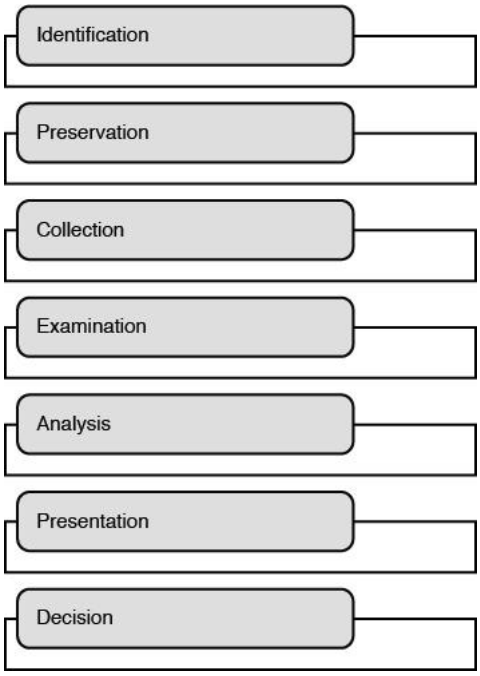

Figura 7-1 Proceso de investigación forense

Las siguientes secciones cubren estos pasos de investigación forense en detalle, así como explican los procedimientos forenses, la información y la documentación, IOCE/SWGDE y NIST, la escena del crimen, el MOM, la cadena de custodia, entrevistas y técnicas de investigación.

Identificar pruebas

El primer paso en cualquier investigación forense es identificar y asegurar la escena del crimen e identificar las pruebas. La identificación de la evidencia se realiza mediante la revisión de registros de auditoría, sistemas de monitoreo, análisis de quejas de usuarios y análisis de mecanismos de detección. Inicialmente, los investigadores podrían no estar seguros de qué evidencia es importante. Preservar la evidencia que tal vez no necesites siempre es mejor que desear tener pruebas de que no conservaste.

Identificar la escena del crimen también es parte de este paso. En las investigaciones digitales, el sistema atacado se considera la escena del crimen. En algunos casos, el sistema del que se originó el ataque también puede considerarse parte de la escena del crimen. Sin embargo, capturar completamente los sistemas del atacante no siempre es posible. Por este motivo, debe asegurarse de capturar los datos que pueden apuntar a un sistema específico, como la captura de direcciones IP, nombres de usuario y otros identificadores.

Preservar y recopilar pruebas

Los siguientes pasos en las investigaciones forenses incluyen preservar y recopilar pruebas. Esto implica hacer imágenes del sistema, implementar la cadena de custodia (que se discute en detalle en su propia sección más adelante), documentar las pruebas y registrar marcas de tiempo.

Antes de recopilar cualquier evidencia, considere el orden de volatilidad. Esta orden asegura que los investigadores recojan pruebas de los componentes que

son más volátiles primero.

El orden de volatilidad es el siguiente:

1. Contenido de memoria
2. Intercambiar archivos
3. Procesos de red
4. Procesos del sistema
5. Información del sistema de archivos
6. Bloques de disco sin procesar

Para crear imágenes del sistema, debe utilizar una herramienta que cree una copia de nivel de bits del sistema. En la mayoría de los casos, debe aislar el sistema y eliminarlo de producción para crear esta copia de nivel de bits. Debe asegurarse de que se conservan dos copias de la imagen. Se almacenará una copia de la imagen para garantizar que una copia precisa y sin daños esté disponible como evidencia. La otra copia se utilizará durante los pasos de examen y análisis. Los resumens de mensajes deben usarse para garantizar la integridad de los datos.

Aunque la imagen del sistema suele ser la prueba más importante, no es la única prueba que necesita. También es posible que deba capturar datos almacenados en caché, tablas de procesos, memoria y el Registro. Al documentar un ataque informático, debe usar un bloc de notas enlazado para mantener notas.

Recuerde que el uso de expertos en investigaciones digitales para asegurar que las pruebas se conservan y recopilan correctamente podría ser necesario. Los investigadores suelen montar un kit de campo para ayudar en el proceso de investigación. Este kit puede incluir etiquetas y etiquetas, herramientas de desmontaje y embalajes de prueba de manipulación. Los kits de campo comerciales están disponibles o podría ensamblar los suyos propios en función de las necesidades de la organización.

Examinar y analizar pruebas

Después de que las pruebas han sido preservadas y recopiladas, el investigador entonces necesita examinar y analizar las pruebas. Durante el examen de las pruebas, cualquier característica, como marcas de tiempo y propiedades de identificación, debe determinarse y documentarse. Después de que la evidencia haya sido analizada completamente utilizando métodos científicos, el incidente completo debe ser reconstruido y documentado.

Hallazgos actuales

Después de un examen y análisis de las pruebas, debe presentarse como prueba en el tribunal. En la mayoría de los casos al presentar pruebas en los tribunales, presentar las conclusiones en un formato que la audiencia puede entender es mejor. Aunque un experto debe ser utilizado para testificar sobre las conclusiones, es importante que el experto sea capaz de articular a una audiencia no técnicas los detalles de las pruebas.

decidir

Al final del proceso judicial, se tomará una decisión sobre la culpabilidad o inocencia de la parte acusada. En ese momento, es posible que ya no sea necesario conservar pruebas, siempre que no exista posibilidad de recurso. Sin embargo, es importante documentar las lecciones aprendidas del incidente. Cualquier persona involucrada en cualquier parte de la investigación debe ser parte de esta sesión aprendida en lecciones.

Procedimientos forenses

La recopilación de pruebas digitales es más complicada que la recopilación de pruebas físicas y debe ser completada por técnicos e investigadores forenses capacitados. Estas personas deben mantenerse al tanto de las últimas herramientas y tecnologías que se pueden utilizar para investigar un delito informático.

Los técnicos e investigadores deben seguir los procedimientos forenses establecidos para asegurarse de que cualquier evidencia recopilada será admisible en un tribunal. Es responsabilidad del individuo capacitado asegurarse de que los procedimientos que utilizan cumplan con las normas establecidas. Organizaciones, como el Instituto Nacional de Normas y Tecnología (NIST) y la Organización Internacional para la Normalización y la Comisión Electrotécnica Internacional (ISO/IEC), establecen normas que ayudan a guiar a las organizaciones en el establecimiento adecuado de estos y otros procedimientos. Consulte siempre con estas normas antes de realizar cualquier investigación para determinar si los procedimientos sugeridos han cambiado o si hay nuevas herramientas disponibles.

Informes y documentación

Una vez que termine cualquier investigación, los profesionales de la seguridad deben proporcionar informes y documentación a la administración sobre el incidente. Este informe debe presentarse a la administración lo antes posible para que la administración pueda determinar si es necesario implementar controles para evitar el incidente. Esta presentación a la administración a menudo ocurrirá antes de la presentación de cualquier hallazgo legal en un tribunal de justicia. Las organizaciones deben establecer procedimientos para garantizar que las personas a las que se presenten los informes tengan la autorización adecuada. También puede ser necesario redactar ciertas partes del informe para garantizar que los casos penales no se vean afectados negativamente.

Si bien la presentación de informes internos es importante, los profesionales de la seguridad también deben tener directrices sobre cuándo reportar incidentes a las fuerzas del orden. Cuanto antes esté involucrada la aplicación de la ley, más probable será que las pruebas sean admisibles en un tribunal. Sin embargo, la mayoría de las fuerzas del orden locales no tienen los conocimientos o habilidades para llevar a cabo una investigación digital completa. Si la organización no tiene personal debidamente capacitado, será necesario llamar a un investigador forense para llevar a cabo la investigación. Los profesionales del derecho también deben ser traídos para ayudar.

La documentación adecuada debe mantenerse a lo largo de la investigación e incluir registros, formularios de cadena de custodia y procedimientos y directrices documentados.

IOCE/SWGDE y NIST

La Organización Internacional de Pruebas Informáticas (IOCE) y el Grupo de Trabajo Científico sobre Evidencia Digital (SWGDE) son dos grupos que estudian la ciencia forense digital y ayudan a establecer normas para las investigaciones digitales. Ambos grupos publican directrices sobre muchos formatos de información digital, incluidos datos informáticos, datos de dispositivos móviles, datos de sistemas informáticos de automóviles, etc. Cualquier investigadores debe asegurarse de que cumplen con los principios de estos grupos.

Si bien la IOCE ya no es un órgano de pruebas funcional, establecieron algunos principios que todavía son aplicables hoy en día. Los principios principales documentados por la IOCE son los siguientes:

- Las normas generales de la prueba deben aplicarse a todas las pruebas digitales.
- Al incautar pruebas digitales, las medidas adoptadas no deben cambiar esa evidencia.
- Cuando una persona necesita acceder a la evidencia digital original, esa persona debe ser entrenada adecuadamente para el propósito.
- Toda actividad relacionada con la incautación, el acceso, el almacenamiento o la transferencia de pruebas digitales debe estar plenamente documentada, preservada y disponible para su revisión.
- Un individuo es responsable de todas las acciones tomadas con respecto a las pruebas digitales mientras las pruebas digitales están en su poder.
- Cualquier agencia que se apodere, acceda, almacenes o transfiera evidencia digital es responsable del cumplimiento de los principios de IOCE.

NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response", proporciona directrices sobre la recopilación de datos, el examen, el análisis y la presentación de informes relacionados con los forenses digitales. Explica el uso de investigadores forenses, personal de TI y controladores de incidentes como parte de cualquier investigación forense. Analiza cómo el costo, el tiempo de respuesta y la sensibilidad de los datos deben afectar cualquier investigación forense.

> **nota**
>
> Nist SP 800-86 se discute con más detalle más adelante en la sección "Normas de laindustria"de este capítulo.

Escena del crimen

Una escena del crimen es el entorno en el que existen pruebas potenciales. Una vez identificada la escena del crimen, se deben tomar medidas para garantizar que el entorno esté protegido, incluido el entorno físico y virtual. Para asegurar la escena del crimen físico, un investigador podría necesitar aislar los sistemas involucrados quitándolos de una red. Sin embargo, los sistemas NO deben apagarse hasta que el investigador esté seguro de que todas las pruebas digitales han sido capturadas. Recuerde: Los datos del equipo en vivo son dinámicos y posiblemente se almacenan en varias ubicaciones volátiles.

Al responder a un posible delito, es importante asegurarse de que el entorno de la escena del crimen está protegido siguiendo los siguientes pasos:

1. Identifique la escena del crimen.
2. Protege toda la escena del crimen.
3. Identificar cualquier evidencia o posible fuente de evidencia que forme parte de la escena del crimen.
4. Recoge todas las pruebas en la escena del crimen.
5. Minimice la contaminación asegurando y preservando adecuadamente todas las pruebas.

Recuerde que puede haber más de una escena del crimen, especialmente en crímenes digitales. Si un atacante infringe la red de una organización, todos los activos que se vieron comprometidos forman parte de la escena del crimen y los activos que utilizó el atacante también forman parte de la escena del crimen.

El acceso a la escena del crimen debe estar estrictamente controlado y limitado sólo a individuos que son vitales para la investigación. Como parte del proceso de documentación, asegúrese de anotar a cualquier persona que tenga acceso a la escena del crimen. Después de que una escena del crimen está contaminada, no existe manera de restaurarla a la condición original.

mamá

Documentar el motivo, la oportunidad y los medios (MOM) es la estrategia más básica para determinar a los sospechosos. *El motivo* es por qué se cometió el crimen y quién cometió el crimen. *La oportunidad* es sobre dónde y cuándo ocurrió el crimen. *Los medios* son todo acerca de cómo el crimen fue llevado a cabo por el sospechoso. Cualquier sospechoso que sea considerado debe poseer las tres cualidades. Por ejemplo, un sospechoso podría tener un motivo para un crimen (ser despedido de la organización) y una oportunidad para cometer el delito (las cuentas de usuario no fueron desactivadas correctamente) pero podría no poseer los medios para llevar a cabo el crimen.

Entender mom puede ayudar a cualquier investigador a reducir la lista de sospechosos.

Cadena de custodia

Al principio de cualquier investigación, usted debe hacer las preguntas quién, qué, cuándo, dónde y cómo. Estas preguntas pueden ayudarle a obtener todos los datos necesarios para la cadena de custodia. La cadena de custodia muestra quién controlaba las pruebas, quién obtuvo las pruebas y quién obtuvo las pruebas. Se debe preservar una cadena de custodia adecuada para procesar con éxito a un sospechoso. Para preservar una cadena de custodia adecuada, las pruebas deben recopilarse siguiendo procedimientos predefinidos de acuerdo con todas las leyes y regulaciones.

Los formularios de cadena de custodia deben utilizarse para rastrear quién tiene acceso a las pruebas, cuándo se produce ese acceso y otros detalles valiosos basados en las necesidades de la organización o la investigación. Esta cadena de custodia debe mantenerse con las pruebas en todo momento. Por ejemplo, si un investigador forense planea analizar el contenido de un registro digital, el investigador forense debe completar la información apropiada en el formulario de cadena de custodia para indicar cuándo el investigador forense obtuvo una copia del registro digital, el tipo de análisis que se está realizando y otros detalles.

El objetivo principal de la cadena de custodia es garantizar que las pruebas son admisibles en los tribunales. Los agentes de la ley hacen hincapié en la cadena de custodia en cualquier investigación que lleven a cabo. Involucrar a las fuerzas del orden al principio del proceso durante una investigación puede ayudar a garantizar que se siga la cadena de custodia adecuada.

Entrevistando

Una investigación a menudo implica entrevistar a sospechosos y testigos. Una persona debe estar a cargo de todas las entrevistas. Porque es necesario obtener pruebas, asegurarse de que el entrevistador entiende qué información debe obtenerse y todas las preguntas a cubrir son importantes. Leer a un sospechoso de sus derechos SÓLO es necesario si las fuerzas del orden están realizando la entrevista. Grabar la entrevista podría ser una buena idea para proporcionar corroboración más adelante cuando la entrevista se utiliza como evidencia.

Si un empleado es sospechoso de un delito informático, un representante del departamento de recursos humanos debe estar involucrado en cualquier interrogatorio del sospechoso. El empleado sólo debe ser entrevistado por una persona que es senior para ese empleado.

Técnicas de investigación

Un crimen informático implica el uso de técnicas de investigación, que incluyen entrevistas (discutidas anteriormente), vigilancia, forenses y operaciones encubiertas.

La vigilancia incluye vigilancia física y vigilancia informática. La vigilancia física utiliza cámaras de seguridad, escuchas telefónicas y seguimiento visual para monitorear el movimiento. La vigilancia informática supervisa los elementos de uso de computadoras y comportamiento en línea. También puede incluir operaciones de picadura, como la instalación de una honeypot o honeynet.

Una vez que se completen las entrevistas y la vigilancia reúna suficientes pruebas, los investigadores querrán realizar análisis forenses avanzados. Las organizaciones pueden hacerlo monitoreando continuamente la actividad, pero si las fuerzas del orden están involucradas, será necesario obtener una orden judicial que permita el análisis forense de computadoras y dispositivos identificados. Los investigadores deben seguir el rastro electrónico dondequiera que conduzca, buscando huellas digitales en correos electrónicos, archivos e historiales de navegación web.

En algunos casos, los crímenes pueden requerir que los investigadores vayan encubiertos, adoptando personajes falsos en línea para atrapar criminales. En este caso, los investigadores deben registrar todas las interacciones como evidencia e incluso pueden organizar una reunión cara a cara para arrestar al perpetrador.

Recolección y manejo de pruebas

Para que las pruebas sean admisibles, deben ser pertinentes, jurídicamente permisibles, fiables, debidamente identificadas y debidamente conservadas. *Lo pertinente* significa que debe probar un hecho material relacionado con el delito en el que se demuestre que se ha cometido un delito, puede proporcionar información que describa el crimen, puede proporcionar información sobre los motivos del autor o puede verificar lo ocurrido.

Legalmente permisible significa que el juez considera que las pruebas son útiles para ayudar al jurado o juez a tomar una decisión y no pueden ser objetadas sobre la base de que son irrelevantes, inmateriales o violan las reglas contra los rumores y otras objeciones. *La fiabilidad* significa que no ha sido manipulado ni modificado. *Debidamente identificado* significa que las pruebas se etiquetan apropiadamente y se introducen en el registro de pruebas. *La preservación* significa que la evidencia no está sujeta a daños o destrucción.

Todas las pruebas deben ser etiquetadas. Al crear etiquetas de evidencia, asegúrese de documentar el modo y los medios de transporte, una descripción completa de la evidencia, incluida la calidad, quién recibió las pruebas y quién tuvo acceso a las pruebas.

Cualquier investigador debe asegurarse de que las pruebas se adhieren a las cinco reglas de la evidencia (ver la siguiente sección). Además, el investigador debe entender cada tipo de evidencia que se puede obtener y cómo se puede utilizar cada tipo en la corte. Los investigadores deben seguir las directrices de vigilancia, búsqueda e incautación. Por último, los investigadores deben comprender las diferencias entre el análisis de medios, software, red y hardware/dispositivo integrado.

Cinco reglas de prueba

Al reunir pruebas, un investigador debe asegurarse de que las pruebas cumplen con las cinco reglas que la rigen:

- Sé auténtico.
- Sé preciso.
- Sé completo.
- Sé convincente.
- Sé admisible.

Debido a que la evidencia digital es más volátil que otras pruebas, todavía debe cumplir con estas cinco reglas.

Tipos de evidencia

Un investigador debe estar al tanto de los tipos de pruebas utilizadas en la corte para asegurarse de que todas las pruebas son admisibles. A veces, el tipo de evidencia determina su admisibilidad.

Los tipos de evidencia que debe comprender son los siguientes:

- La mejor evidencia
- Pruebas secundarias
- Pruebas directas
- Pruebas concluyentes
- Pruebas circunstanciales
- Pruebas corroborativas
- Pruebas de opinión
- Pruebas de rumores

La mejor evidencia

La regla de la mejor prueba establece que cuando se presenten pruebas, como un documento o una grabación, sólo se aceptará el original a menos que exista una razón legítima de por qué no se puede utilizar el original. En la mayoría de los casos, la evidencia digital no se considera la mejor evidencia porque los investigadores deben capturar *copias* de los datos originales y el estado.

Sin embargo, los tribunales pueden aplicar la mejor regla de pruebas a las pruebas digitales caso por caso, dependiendo de las pruebas y la situación. En esta situación, la copia debe ser probada por un testigo experto que puede testificar sobre el contenido y confirmar que se trata de una copia precisa del original.

Pruebas secundarias

Las pruebas secundarias se han reproducido de un original o se han sustituido por un elemento original. Las copias de documentos originales y testimonio oral se consideran pruebas secundarias.

Pruebas directas

La evidencia directa prueba o refuta un hecho a través del testimonio oral basado en la información recopilada a través de los sentidos del testigo. Un testigo puede testificar sobre lo que vio, olió, escuchó, probó o sintió. Esto se considera evidencia directa. Sólo el testigo puede dar pruebas directas. Nadie más puede informar sobre lo que el testigo les dijo porque eso se considera evidencia de rumores.

Pruebas concluyentes

Las pruebas concluyentes no requieren ninguna otra corroboración y no pueden ser contradichos por ninguna otra prueba.

Evidencia circunstancial

Las pruebas circunstanciales proporcionan inferencia de información de otros hechos relevantes intermedios. Esta evidencia ayuda a un jurado a llegar a una conclusión mediante el uso de un hecho para dar a entender que otro hecho es verdadero o falso. Un ejemplo está dando a entender que un ex empleado cometió un acto contra una organización debido a su aversión a la organización después de su despido.

Pruebas corroborativas

Las pruebas corroborativas respaldan otra prueba. Por ejemplo, si un sospechoso produce un recibo para probar que estaba en un restaurante en particular en un momento determinado y luego una camarera testifica que esperó al sospechoso en ese momento, entonces la camarera proporciona pruebas corroborantes a través de su testimonio.

Pruebas de opinión

Las pruebas de opinión se basan en lo que el testigo piensa, siente o infiere con respecto a los hechos. Sin embargo, si se utiliza un testigo experto, esa experta puede testificar sobre un hecho basado en sus conocimientos en un área determinada. Por ejemplo, un psiquiatra puede testificar sobre las conclusiones sobre el estado mental de un sospechoso. El testimonio de expertos no se considera evidencia de opinión debido al conocimiento y la experiencia del experto.

Evidencia de rumores

La evidencia de Hearsay es una evidencia que es de segunda mano, donde el testigo no tiene conocimiento directo del hecho afirmado, pero sólo lo sabe por ser dicho por alguien. En algunos casos, las pruebas basadas en computadoras se consideran rumores, especialmente si un experto no puede testificar sobre la exactitud e integridad de las pruebas.

Vigilancia, búsqueda e incautación

La vigilancia, la búsqueda y la incautación son facetas importantes de cualquier investigación. La vigilancia es el acto de monitorear el comportamiento, las actividades u otra información cambiante, generalmente de las personas. La búsqueda es el acto de perseguir elementos o información. La incautación es el acto de tomar la custodia de componentes físicos o digitales.

Dos tipos de vigilancia son utilizados por los investigadores: vigilancia física y vigilancia informática. La vigilancia física ocurre cuando las acciones de una persona son reportadas o capturadas usando cámaras, observancia directa o televisión de circuito cerrado (CCTV). La vigilancia informática se produce cuando las acciones de una persona se notifican o capturan mediante información digital, como registros de auditoría.

En la mayoría de los casos se requiere una orden de registro para buscar activamente en un sitio privado en busca de pruebas. Para que se emita una

orden de registro, la causa probable de que se haya cometido un delito debe ser probada ante un juez. También se debe corroborar al juez la existencia de pruebas. La única vez que no es necesario emitir una orden de registro es en circunstancias exigentes, que son circunstancias de emergencia necesarias para prevenir daños físicos, la destrucción de pruebas, la fuga del sospechoso o alguna otra consecuencia que frustra indebidamente los esfuerzos legítimos de aplicación de la ley. Las circunstancias exigentes tendrán que ser probadas cuando las pruebas se presenten en los tribunales.

La incautación de pruebas sólo puede ocurrir si las pruebas se enumeran específicamente como parte de la orden de registro a menos que las pruebas estén a la vista. Se pueden incautar pruebas específicamente enumeradas en la orden de registro, y la búsqueda sólo puede ocurrir en áreas específicamente enumeradas en la orden judicial.

Las reglas de búsqueda e incautación no se aplican a organizaciones privadas e individuos. La mayoría de las organizaciones advierten a sus empleados que los archivos almacenados en los recursos de la organización se consideran propiedad de la organización. Esto suele ser parte de cualquier política de no expectativa de privacidad.

Una discusión de pruebas sería incompleta sin discutir la jurisdicción. Debido a que los delitos informáticos pueden implicar activos que cruzan los límites jurisdiccionales, los investigadores deben entender que las leyes civiles y penales de los países pueden diferir mucho. Siempre es mejor consultar al personal de las fuerzas del orden locales para cualquier investigación criminal o civil y seguir cualquier consejo que den para las investigaciones que crucen jurisdicciones.

Análisis de medios

Los investigadores pueden realizar muchos tipos de análisis de medios, dependiendo del tipo de medio. Un especialista en recuperación de medios puede ser empleado para proporcionar una imagen forense certificada, que es un proceso costoso.

Se pueden utilizar los siguientes tipos de análisis de medios:

- **Imágenes de disco:** Crea una imagen exacta del contenido del disco duro.
- **Análisis de espacio flojo:** Analiza el espacio flojo (marcado como vacío o reutilizable) en la unidad para ver si se pueden recuperar datos antiguos (marcados para su eliminación).
- **Análisis de contenido:** Analiza el contenido de la unidad y proporciona un informe que detalla los tipos de datos por porcentaje.

- **Análisis de esteganografía:** Analiza los archivos de una unidad para ver si los archivos han sido alterados o para detectar el cifrado utilizado en el archivo.

Análisis de software

El análisis de software es un poco más difícil de realizar que el análisis de medios porque a menudo requiere la entrada de un experto en código de software, incluido el código fuente, el código compilado o el código de máquina. A menudo implica descompilación o ingeniería inversa. Este tipo de análisis se utiliza a menudo durante el análisis de malware y disputas de derechos de autor.

Las técnicas de análisis de software incluyen lo siguiente:

- **Análisis de contenido:** Analiza el contenido del software, particularmente el malware, para determinar para qué propósito se creó el software.
- **Ingeniería inversa:** Recupera el código fuente de un programa para estudiar cómo realiza el programa determinadas operaciones.
- **Identificación del autor:** Intenta determinar el autor del software.
- **Análisis de contexto:** Analiza el entorno en el que se encontró el software para descubrir pistas para determinar el riesgo.

análisis de redes

El análisis de red implica el uso de herramientas de red para conservar registros y actividad en busca de pruebas.

Las técnicas de análisis de red incluyen lo siguiente:

- **Análisis de comunicaciones:** Analiza la comunicación a través de una red capturando la totalidad o parte de la comunicación y buscando determinados tipos de actividad.
- **Análisis de registros:** Analiza los registros de tráfico de red.
- **Trazado de trazado:** Traza la trayectoria de un paquete de tráfico o tipo de tráfico determinado para descubrir la ruta utilizada por el atacante.

Análisis de hardware/dispositivo integrado

El análisis de hardware/dispositivo integrado implica el uso de las herramientas y el firmware proporcionados con los dispositivos para

determinar las acciones que se realizaron en y por el dispositivo. Las técnicas utilizadas para analizar el hardware/dispositivo integrado varían en función del dispositivo. En la mayoría de los casos, el proveedor de dispositivos puede proporcionar asesoramiento sobre la mejor técnica para usar dependiendo de la información que necesite. El análisis de registros, el análisis del sistema operativo y las inspecciones de memoria son algunas de las técnicas generales utilizadas.

Este tipo de análisis se utiliza cuando se analizan los dispositivos móviles. Para realizar este tipo de análisis, NIST realiza las siguientes recomendaciones:

- Cualquier análisis no debe cambiar los datos contenidos en el dispositivo o los medios de comunicación.
- Sólo los investigadores competentes deben acceder a los datos originales y deben explicar todas las acciones que tomaron.
- Los registros de auditoría u otros registros deben crearse y conservarse durante todos los pasos de la investigación.
- El investigador principal es responsable de garantizar que se sigan todos estos procedimientos.
- Todas las actividades relativas a las pruebas digitales, incluida su incautación, el acceso a ella, su almacenamiento o su transferencia, deben documentarse, conservarse y estar disponibles para su revisión.

Herramientas, tácticas y procedimientos forenses digitales

Para la recolección de pruebas, los investigadores necesitarán un kit de herramientas digital. Se debe incluir lo siguiente como parte de cualquier kit de herramientas digital:

- Computadoras portátiles forenses y fuentes de alimentación
- Conjuntos de herramientas
- cámara digital
- Carpeta de casos
- Formularios en blanco
- Recolección de pruebas y suministros de embalaje
- software
- Tarjeta aérea para acceso a Internet
- Cables para transferencia de datos (red, crossover, USB, etc.)
- Discos duros en blanco y otros medios

- Bloqueadores de escritura de hardware

El kit de herramientas digitales debe contener herramientas forenses que permitan a un investigador obtener datos que se pueden utilizar como evidencia. Las herramientas utilizadas por los investigadores se clasifican según el tipo de información que obtienen, como se muestra en la siguiente lista:

- Herramientas de captura de discos y datos
- Visores de archivos
- Herramientas de análisis de archivos
- Herramientas de análisis de registros
- Herramientas de análisis de Internet
- Herramientas de análisis de correo electrónico
- Herramientas de análisis de dispositivos móviles
- herramientas de análisis de macOS
- Herramientas forenses de la red
- Herramientas forenses de base de datos

Muchas de las herramientas disponibles hoy en día pueden proporcionar servicios en varias áreas enumeradas anteriormente. Los investigadores deben obtener capacitación en el uso adecuado de estas herramientas.

Las herramientas que se pueden incluir en un kit de herramientas forenses digitales incluyen lo siguiente:

- Marco Forense Digital (DFF)
- Arquitectura forense de computadora abierta (OCFA)
- Entorno INvestigative asistido por ordenador (CAINE)
- Radiografías forenses
- Kit de herramientas forenses de investigación de SANS (SIFT)
- Encase Forense
- Reconocimiento del Registro
- El kit de autenticación (TSK)
- LibForensics

- volatilidad
- WindowsSCOPE
- El kit de herramientas del forense (TCT)
- Suite forense de oxígeno
- Bulk_Extractor
- Xplico
- Redline
- Extractor de pruebas forenses en línea por computadora (COFEE)
- Claridad
- XRY
- Hélice3
- UFED

Los investigadores también deben estar familiarizados con las tácticas y procedimientos forenses digitales adecuados que se utilizan comúnmente. Por esta razón, los investigadores deben estar debidamente capacitados para asegurarse de que se siguen las herramientas, tácticas y procedimientos para que las pruebas recopiladas sean admisibles en los tribunales. Tenga en cuenta que usted no debe ser probado en la funcionalidad de las herramientas individuales o las tácticas y procedimientos forenses digitales en el examen CISSP; sin embargo, debe entender que estas herramientas, tácticas y procedimientos proporcionan automatización de la investigación forense digital y cumplimiento de los estándares de investigación. El papel laboral de un candidato del CISSP no se define como la realización de tareas individuales de investigación forense; sin embargo, el profesional del CISSP debe estar familiarizado con las herramientas, tácticas y procedimientos disponibles para garantizar que el investigador de una organización obtenga las herramientas adecuadas para realizar investigaciones digitales y siga las tácticas y procedimientos apropiados.

TIPOS DE INVESTIGACIÓN

Se pide a los profesionales de la seguridad que investiguen cualquier incidente que ocurra. Como resultado de los diferentes activos que se ven afectados, los profesionales de la seguridad deben ser capaces de realizar diferentes tipos de investigaciones, incluyendo operaciones / administrativas, penales, civiles, regulatorias, estándar de la industria, y investigaciones de exhibición electrónica. Estos tipos de investigación se describen en las secciones siguientes.

Operaciones/Administrativo

Las investigaciones administrativas son investigaciones que no dan lugar a ningún problema penal, civil o reglamentario. Las investigaciones administrativas también pueden denominarse *investigaciones de operaciones*. En la mayoría de los casos, este tipo de investigación se completa para determinar la causa raíz de un incidente para que se puedan tomar medidas para evitar que este incidente vuelva a ocurrir en el futuro. Este proceso se conoce como *análisis de causa raíz*. Debido a que no se ha violado ninguna ley penal, civil o reglamentaria, no es tan importante documentar las pruebas. Sin embargo, los profesionales de la seguridad todavía deben tomar medidas para documentar las lecciones aprendidas.

Como ejemplo de este tipo de investigación, supongamos que a un usuario se le asignan permisos inapropiados en función de su rol de trabajo. Si esto fuera el resultado de una acción criminal, debería ocurrir una investigación criminal. Sin embargo, esto podría haber ocurrido simplemente a través de errores cometidos por el personal. Debido a que un profesional de la seguridad no sabría la causa de los permisos inapropiados, tendría que iniciar la investigación siguiendo las directrices forenses adecuadas. Sin embargo, una vez que determinó que el incidente fue el resultado de un accidente, ya no sería necesario seguir esas directrices. Cualquier persona que lleve a cabo este tipo de investigación debe asegurarse de que se realicen los cambios adecuados para evitar que un incidente de este tipo vuelva a ocurrir, incluida la puesta en marcha de controles de seguridad. En el caso del ejemplo de permisos inapropiados, el profesional de seguridad podría encontrar que la plantilla de cuenta de usuario que se usó para crear la cuenta de usuario se asignó a un grupo inapropiado y, por lo tanto, debe asegurarse de que se revisa la plantilla de cuenta de usuario.

Criminal

Las investigaciones criminales son investigaciones que se llevan a cabo porque se ha violado una ley federal, estatal o local. En este tipo de investigación, una organización debe asegurarse de que las fuerzas del orden participen en la investigación lo antes posible para garantizar que el delito pueda ser debidamente documentado, investigado y procesado. Las investigaciones criminales dan lugar a un juicio penal.

civil

Una investigación civil ocurre cuando una organización o parte sospecha de otra organización de actos civiles. Por ejemplo, si una organización sospecha que otra organización violó un derecho de autor, se podría presentar una demanda civil. Si bien los casos penales de derechos de autor ocurren, sólo pueden ser presentados por fiscales del gobierno. En un caso civil, la organización debe asegurarse de que se cumplan todas las reglas de pruebas y de que la representación legal esté involucrada como parte de la investigación.

regulador

Una investigación regulatoria se produce cuando un organismo regulador investiga a una organización por una infracción reglamentaria. En la historia reciente, la Securities and Exchange Commission (SEC) ha llevado a cabo muchas investigaciones regulatorias con respecto a las organizaciones y sus operaciones financieras. Independientemente del organismo regulador que esté llevando a cabo la investigación, se notificará a la organización que se está investigando que se está llevando a cabo una investigación. La organización debe contar con políticas y directrices para garantizar el pleno cumplimiento de la investigación. El incumplimiento de dicha investigación puede dar lugar a que se presenten cargos contra la organización y cualquier personal involucrado.

Normas de la industria

Tal como se define en capítulos anteriores, las normas establecen criterios dentro de una industria relativos al funcionamiento estándar y a la realización de operaciones en sus respectivos campos de producción. En los forenses digitales, las normas proporcionan los requisitos generalmente aceptados seguidos por los investigadores digitales.

Las organizaciones deben investigar los estándares forenses digitales disponibles, incluidos los de NIST e ISO/IEC. NIST SP 800-86 proporciona directrices para integrar técnicas forenses en la respuesta a incidentes.

Para establecer una capacidad forense organizativa, NIST SP 800-86 proporciona las siguientes directrices:

- Las organizaciones deben tener la capacidad de realizar análisis forenses de computadoras y redes.
- Las organizaciones deben determinar qué partes deben manejar cada aspecto de los forenses.
- Los equipos de manejo de incidentes deben tener capacidades forenses sólidas.
- Muchos equipos dentro de una organización deben participar en los forenses.
- Las consideraciones forenses deben abordarse claramente en las políticas.
- Las organizaciones deben crear y mantener directrices y procedimientos para realizar tareas forenses.

Según NIST SP 800-86, las fases básicas del proceso forense son la recopilación, el examen, el análisis y la presentación de informes. Esto difiere ligeramente del proceso notificado anteriormente. En algunos casos, los dos primeros pasos presentados anteriormente (identificación y preservación) se consideran parte de la respuesta a incidentes, pero no parte del proceso forense en sí. Sin embargo, las cuatro fases del NIST SP 800-86 corresponden

a los pasos 3 a 7 del proceso anterior. La Figura 7-2 muestra el proceso forense a medida que transforma los medios en evidencia, si se necesitan pruebas para la aplicación de la ley o para el uso interno de una organización.

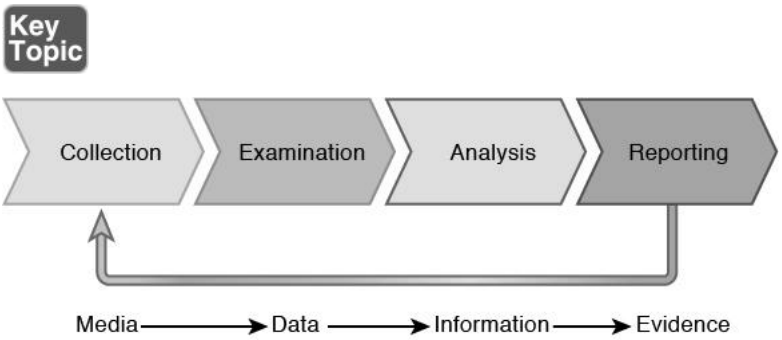

Figura 7-2 Proceso forense NIST SP 800-86 (Imagen cortesía de NIST)

Durante la recopilación, los datos relacionados con un evento específico se identifican, etiquetan, registran y recopilan, y se conserva su integridad. En la segunda fase, se ejecutan herramientas y técnicas forenses adecuadas a los tipos de datos que se recopilaron para identificar y extraer la información pertinente de los datos recopilados y proteger su integridad. El examen puede utilizar una combinación de herramientas automatizadas y procesos manuales. La siguiente fase, el análisis, consiste en analizar los resultados del examen para obtener información útil que aborde las preguntas que fueron el impulso para realizar la recopilación y el examen. La fase final consiste en informar de los resultados del análisis, que puede incluir la descripción de las acciones realizadas, la determinación de qué otras acciones deben realizarse y la recomendación de mejoras en las políticas, directrices, procedimientos, herramientas y otros aspectos del proceso forense.

Las recomendaciones clave para el proceso forense son las siguientes:

- Las organizaciones deben realizar análisis forenses mediante un proceso coherente.
- Los analistas deben ser conscientes de la gama de posibles fuentes de datos.
- Las organizaciones deben ser proactivas en la recopilación de datos útiles.
- Los analistas deben realizar la recopilación de datos mediante un proceso estándar.
- Los analistas deben utilizar un enfoque metódico para estudiar los datos.
- Los analistas deben revisar sus procesos y prácticas.

NIST SP 800-86 proporciona directrices para el uso de datos de archivos de datos, sistemas operativos, tráfico de red y aplicaciones. Las recomendaciones clave presentadas para utilizar datos de archivos de datos son las siguientes:

- Los analistas deben examinar copias de archivos, no los archivos originales.
- Los analistas deben conservar y verificar la integridad del archivo.
- Los analistas deben confiar en encabezados de archivo, no en extensiones de archivo, para identificar tipos de contenido de archivo.
- Los analistas deben tener un kit de herramientas forense para el examen y análisis de datos.

Las recomendaciones clave presentadas para utilizar datos de los sistemas operativo son las siguientes:

- Los analistas deben actuar adecuadamente para preservar los datos volátiles del sistema operativo.
- Los analistas deben usar un kit de herramientas forense para recopilar datos volátiles del sistema operativo.
- Los analistas deben elegir el método de apagado adecuado para cada sistema.

Las recomendaciones clave presentadas para utilizar datos del tráfico de red son las siguientes:

- Las organizaciones deben tener políticas con respecto a la privacidad y la información confidencial.
- Las organizaciones deben proporcionar almacenamiento adecuado para los registros relacionados con la actividad de red.
- Las organizaciones deben configurar orígenes de datos para mejorar la recopilación de información.
- Los analistas deben tener conocimientos técnicos razonablemente completos.
- Los analistas deben considerar la fidelidad y el valor de cada fuente de datos.
- Por lo general, los analistas deben centrarse en las características y el impacto del evento.

Las recomendaciones clave presentadas para el uso de datos de aplicaciones son las siguientes:

- Los analistas deben considerar todas las fuentes de datos de aplicaciones posibles.
- Los analistas deben reunir datos de aplicaciones de varias fuentes.

Las recomendaciones clave presentadas para utilizar datos de varios orígenes son las siguientes:

- Los analistas pueden manejar muchas situaciones de manera más eficaz mediante el análisis de varias fuentes de datos individuales y luego correlacionar eventos entre ellos.
- Las organizaciones deben ser conscientes de la complejidad técnica y logística del análisis.

Exhibición electrónica

*El descubrimiento electrónico (eDiscovery)*se refiere a litigios o investigaciones gubernamentales que se ocupan del intercambio de información en formato electrónico como parte del proceso de descubrimiento. Implica información almacenada electrónicamente (ESI) e incluye correos electrónicos, documentos, presentaciones, bases de datos, correo de voz, archivos de audio y video, redes sociales y sitios web. Los profesionales de la seguridad deben asegurarse de que el contenido original y los metadatos de ESI se conserven para evitar reclamaciones de polinización o manipulación de pruebas más adelante en el litigio. Una vez que se recopila el ESI adecuado, debe mantenerse en un entorno seguro para su revisión.

ACTIVIDADES DE REGISTRO Y MONITOREO

Como parte de la seguridad de las operaciones, los administradores deben asegurarse de que las actividades del usuario se registran y supervisan con regularidad. Esto incluye auditoría y revisión, detección y prevención de intrusiones, información de seguridad y gestión de eventos, monitoreo continuo y monitoreo de egresos.

Auditoría y revisión

La rendición de cuentas es imposible sin un registro de las actividades y la revisión de esas actividades. Los registros de auditoría de captura y supervisión proporcionan la prueba digital cuando es alguien que está realizando ciertas actividades debe ser identificado. Esto va tanto para los buenos como para los malos. En muchos casos se requiere determinar quién configuró mal algo en lugar de quién robó algo. Los rastros de auditoría basados en códigos de acceso e identificación establecen la responsabilidad individual. Las preguntas que se deben abordar al revisar los registros de auditoría incluyen las siguientes:

- ¿Los usuarios acceden a información o realizan tareas innecesarias para sus trabajos?
- ¿Se están cometiendo errores repetitivos (como eliminaciones) ?
- ¿Demasiados usuarios tienen derechos y privilegios especiales?

El nivel y la cantidad de auditoría deben reflejar la política de seguridad de la empresa. Las auditorías pueden ser autopresuficiencias o realizadas por un tercero. Las auto-auditorías siempre introducen el peligro de subjetividad en el proceso. Los registros se pueden generar en una amplia variedad de dispositivos, incluidos los sistemas de detección de intrusiones (IDS), servidores, enrutadores e switches. De hecho, un IDS basado en host hace uso de los registros del sistema operativo del equipo host.

Al evaluar controles sobre registros o registros de auditoría, aborde las siguientes preguntas:

- ¿El seguimiento de auditoría proporciona un seguimiento de las acciones del usuario?
- ¿Está estrictamente controlado el acceso a los registros en línea?
- ¿Hay separación de funciones entre el personal de seguridad que administra la función de control de acceso y los que administran la pista de auditoría?

Mantenga y almacene los registros de acuerdo con la directiva de retención definida en la directiva de seguridad de la organización. Deben estar asegurados para evitar modificaciones, eliminación y destrucción. Cuando la auditoría funciona en un rol de supervisión, admite la función de seguridad *de detección* en la categoría *técnica*. Cuando se lleva a cabo la revisión formal de los registros de auditoría, es una forma de control *administrativo de detectives*. La revisión de los datos de auditoría debe ser una función independiente de la administración diaria del sistema.

Tipos de registro

El registro es el proceso de registrar la información del evento en un archivo de registro o base de datos. Captura eventos del sistema, cambios, mensajes y otra información que muestran las actividades que se producen en un sistema o dispositivo. Los diferentes tipos de registros que usan los profesionales de seguridad incluyen registros de seguridad, registros de sistemas, registros de aplicaciones, registros de firewall, registros de proxy y registros de cambios.

Los registros de seguridad registran el acceso a los recursos, incluido el acceso a archivos, carpetas e impresoras. Pueden grabar cuando un usuario accede, modifica o elimina un archivo o carpeta. Aunque la mayoría de los sistemas registrarán cuando se accede a los archivos clave, a menudo es necesario que un administrador habilite la auditoría en otros recursos, como carpetas de datos o impresoras de red. Cuando la auditoría se ejecuta en un dispositivo, afectará al rendimiento de ese dispositivo. Por este motivo, los profesionales de la seguridad solo deben configurar la auditoría cuando sea necesario en función de las directivas de seguridad de la organización.

Los registros del sistema registran eventos del sistema, como el inicio y apagado del sistema y del servicio. Pueden ayudar a un profesional de la seguridad a determinar las acciones tomadas por un usuario malintencionado.

Las aplicaciones registran las acciones de registro que se producen dentro de una aplicación específica. Los profesionales de seguridad deben trabajar con desarrolladores de aplicaciones o proveedores para determinar qué tipo de información se debe registrar.

Los registros de firewall registran la información de tráfico de red, incluido el tráfico entrante y saliente. Esto normalmente incluye datos importantes, como direcciones IP y números de puerto que se pueden usar para determinar el origen de un ataque.

Los registros de proxy registran los detalles del tráfico de Internet que pasa a través del servidor proxy, incluidos los sitios que visitan los usuarios, cuánto tiempo se pasa en esos sitios y si se intenta acceder a sitios prohibidos.

Los cambios en los registros informan de los cambios realizados en un dispositivo o aplicación específico como parte del proceso de administración de cambios.

Tipos de auditoría

Cuando la auditoría está habilitada, los administradores pueden seleccionar eventos individuales para supervisar para garantizar la responsabilidad del usuario. Los tipos de auditoría incluyen auditorías de revisión de acceso, auditorías de privilegios de usuario y auditorías de grupo con privilegios.

Las auditorías de revisión de acceso garantizan que el acceso a objetos y las prácticas de administración de cuentas de usuario se adhieran a la directiva de seguridad de la organización. Las auditorías de privilegios de usuario supervisan el uso correcto y de permisos para todos los usuarios. Las auditorías de grupo con privilegios supervisan cuándo se usan grupos de alto nivel y cuentas de administrador.

Detección y prevención de intrusiones

Los IDS alertan a las organizaciones cuando se produce acceso o acciones no autorizados, mientras que los sistemas de prevención de intrusiones (IPS) supervisan el mismo tipo de actividad, pero en realidad trabajan para evitar que las acciones se realicen correctamente. Los dispositivos IDS e IPS se pueden utilizar durante las investigaciones para proporcionar información sobre los patrones de tráfico que ocurren justo antes de que un ataque tenga éxito. Los profesionales de seguridad deben ajustar constantemente los dispositivos IDS e IPS para asegurarse de que se detecta o impide la actividad correcta. A medida que se producen cambios en la forma en que se llevan a cabo los ataques, estos sistemas deben ajustarse.

nota

Los dispositivos IDS e IPS se discuten con más detalle más adelante en este capítulo y también en el Capítulo 4,"Comunicación y Seguridad de red."

Información de seguridad y gestión de eventos (SIEM)

SIEM puede recopilar información de registro y sistema para cumplir con los requisitos reglamentarios, proporcionar responsabilidad interna, proporcionar gestión de riesgos y realizar monitoreo y tendencias. SIEM almacena información sin procesar de varios sistemas y dispositivos y agrega esa información a una sola base de datos. Los profesionales de la seguridad deben trabajar juntos para garantizar que se supervisarán las acciones adecuadas y para garantizar que se realicen los exámenes correctos de los registros. Dado que los sistemas SIEM son repositorios centralizados de información de seguridad, las organizaciones deben tener especial cuidado de proporcionar una seguridad adecuada para estos sistemas para garantizar que los atacantes no puedan acceder o modificar los registros contenidos en ellos.

nota

Siem se discute con más detalle en el Capítulo 6,"Evaluación y Pruebas de Seguridad."

Monitoreo continuo

Cualquier actividad de registro y supervisión debe formar parte de un programa de supervisión continua de la organización. El programa de supervisión continua debe diseñarse para satisfacer las necesidades de la organización e implementarse correctamente para garantizar que la infraestructura crítica de la organización esté protegida. Es posible que las organizaciones quieran buscar soluciones de supervisión continua como servicio (CMaaS) implementadas por proveedores de servicios en la nube.

Monitoreo de egresos

La supervisión de salida se produce cuando una organización supervisa el flujo saliente de información de una red a otra. La forma más popular de monitoreo de salida se lleva a cabo utilizando firewalls que monitorean y controlan el tráfico saliente.

La fuga de datos se produce cuando los datos confidenciales se divulgan al personal no autorizado, ya sea intencional o inadvertidamente. El software de prevención de pérdida de datos (DLP) intenta evitar la fuga de datos. Lo hace manteniendo la conciencia de las acciones que se pueden y no se pueden

tomar con respecto a un documento. Por ejemplo, podría permitir la impresión de un documento, pero solo en la oficina de la empresa. También podría no permitir el envío del documento a través de correo electrónico. El software DLP utiliza filtros de entrada y salida para identificar datos confidenciales que salen de la organización y pueden evitar este tipo de fugas.

Otro escenario podría ser la versión de planes de producto que solo deberían estar disponibles para el grupo Ventas. Un profesional de la seguridad podría establecer una política como la siguiente para ese documento:

- No se puede enviar por correo electrónico a nadie que no sea miembros del grupo Sales.
- No se puede imprimir.
- No se puede copiar.

Hay dos ubicaciones donde se puede implementar un DLP:

- **DLP de red:** Instalado en los puntos de salida de red cerca del perímetro, la red DLP analiza el tráfico de red.
- **Punto final DLP:** Endpoint DLP se ejecuta en estaciones de trabajo o servidores de usuario final de la organización.

Puede utilizar métodos precisos e imprecisos para determinar qué es sensible:

- **Métodos precisos:** Estos métodos implican el registro de contenido y desencadenan casi cero incidentes falsos positivos.
- **Métodos imprecisos:** Estos métodos pueden incluir palabras clave, léxicos, expresiones regulares, expresiones regulares extendidas, etiquetas de metadatos, análisis bayesiano y análisis estadístico.

El valor de un sistema DLP reside en el nivel de precisión con el que puede localizar y evitar la fuga de datos confidenciales.

> **nota**
>
> La esteganografía y la marca de agua a veces forman parte del monitoreo de egresos. Ambas herramientas criptográficas se discuten en el Capítulo 3,"Arquitectura de Seguridad e Ingeniería."

PROVISIÓN DE RECURSOS

El aprovisionamiento de recursos es un proceso en las operaciones de seguridad que garantiza que una organización implemente solo los activos que necesita actualmente. El aprovisionamiento de recursos debe seguir el ciclo de

vida de los recursos de la organización. Para administrar correctamente el ciclo de vida de los recursos, una organización debe mantener un inventario de activos preciso y usar los procesos de administración de configuración adecuados. Los recursos que participan en el aprovisionamiento incluyen activos físicos, activos virtuales, activos en la nube y aplicaciones.

Inventario y Gestión de Activos

Un activo es cualquier elemento de valor para una organización, incluidos los dispositivos físicos y la información digital. Reconocer cuándo se roban los activos o se implementan incorrectamente es imposible si no existe ningún recuento de artículos o sistema de inventario o si el inventario no se mantiene actualizado. Todos los equipos deben inventariarse y toda la información relevante sobre cada dispositivo debe mantenerse y mantenerse actualizada. Cada activo debe estar completamente documentado, incluidos los números de serie, los números de modelo, la versión de firmware, la versión del sistema operativo, el personal responsable, etc. La organización debe mantener esta información tanto electrónicamente como en copia impresa. El mantenimiento de este inventario ayudará a determinar cuándo se deben implementar nuevos activos o cuándo se deben retirar los activos desplegados actualmente.

Los dispositivos de seguridad, como firewalls, dispositivos de traducción de direcciones de red (NAT) e IDS e IPS, deben recibir la mayor atención porque se relacionan con la seguridad física y lógica. Más allá de esto, los dispositivos que se pueden robar fácilmente, como computadoras portátiles, tabletas y teléfonos inteligentes, deben ser bloqueados. Si eso no es práctico, considere la posibilidad de bloquear este tipo de dispositivos a objetos estacionarios (por ejemplo, utilizando bloqueos de cable con portátiles).

Cuando la tecnología está disponible, el seguimiento de dispositivos pequeños puede ayudar a mitigar la pérdida de ambos dispositivos y sus datos. Muchos teléfonos inteligentes ahora incluyen software de seguimiento que le permite localizar un dispositivo después de que ha sido robado o perdido mediante el uso de seguimiento de torres celulares o GPS. Implemente esta tecnología cuando esté disponible.

Otra característica útil disponible en muchos teléfonos inteligentes y otros dispositivos portátiles es una función de limpieza remota. Esto permite al usuario enviar una señal a un dispositivo robado, instruyéndole a borrar los datos contenidos en el dispositivo. Del mismo modo, estos dispositivos normalmente también vienen con la capacidad de ser bloqueados remotamente cuando están fuera de lugar.

El control estricto del uso de dispositivos multimedia portátiles puede ayudar a evitar que la información confidencial salga de la red. Esto incluye CDs, DVDs, unidades flash y discos duros externos. Aunque las reglas escritas deben estar en vigor sobre el uso de estos dispositivos, también es posible usar directivas de seguridad para evitar la copia de datos en estos tipos de medios. También es posible permitir la copia de datos en estos tipos de unidad siempre

y cuando los datos se cifran. Si el sistema operativo de red proporciona estas funciones, debe implementarlas.

No debería ser posible que las personas no autorizadas accedan y manipule ningún dispositivo. La manipulación incluye desfigurar, dañar o cambiar la configuración de un dispositivo. Las aplicaciones deben utilizar programas de verificación de integridad para buscar evidencia de manipulación de datos, errores y omisiones.

Cifrar los datos confidenciales almacenados en dispositivos puede ayudar a evitar la exposición de datos en caso de robo o en caso de acceso inapropiado del dispositivo.

Activos físicos

Los activos físicos incluyen servidores, equipos de escritorio, portátiles, dispositivos móviles y dispositivos de red que se implementan en la empresa. Los activos físicos deben implementarse y retirarse en función de las necesidades organizativas. Por ejemplo, supongamos que una organización implementa un Punto de acceso inalámbrico (WAP) para su uso por un auditor externo. El aprovisionamiento adecuado de recursos debe garantizar que el WAP sea dado de baja una vez que el auditor externo ya no necesite acceso a la red. Sin una gestión adecuada del inventario y de la configuración, el WAP puede permanecer desplegado y se puede utilizar en algún momento para llevar a cabo un ataque de red inalámbrica.

Activos virtuales

Los activos virtuales incluyen redes definidas por software, redes de área de almacenamiento virtual (VSAN), sistemas operativos invitados implementados en máquinas virtuales (VM) y enrutadores virtuales. Al igual que con los activos físicos, la implementación y el desmantelamiento de activos virtuales deben controlarse estrictamente como parte de la administración de la configuración porque los activos virtuales, al igual que los activos físicos, pueden verse comprometidos. Por ejemplo, una máquina virtual de Windows 10 implementada en un sistema de Windows Server 2016 solo debe conservarse hasta que ya no sea necesario. Siempre y cuando se use la máquina virtual, es importante asegurarse de que se implementan las actualizaciones, revisiones y controles de seguridad adecuados en ella como parte de la administración de la configuración. Cuando los usuarios ya no tienen acceso a la máquina virtual, se debe quitar.

El almacenamiento virtual se produce cuando el almacenamiento físico de varios dispositivos de almacenamiento de red se compila en un único espacio de almacenamiento virtual. La virtualización de bloques separa el almacenamiento lógico del almacenamiento físico. La virtualización de archivos elimina la dependencia entre los datos a los que se accede en el nivel de archivo y la ubicación de almacenamiento físico de los archivos. El almacenamiento virtual basado en host requiere software que se ejecute en el host. El almacenamiento de información basado en dispositivos de

almacenamiento se ejecuta en un controlador de almacenamiento y permite conectar otros controladores de almacenamiento. El almacenamiento virtual basado en red utiliza dispositivos basados en red, como iSCSI o Fibre Channel, para crear una solución de almacenamiento.

Activos en la nube

Los activos en la nube incluyen servicios en la nube, máquinas virtuales, redes de almacenamiento y otros servicios en la nube contratados a través de un proveedor de servicios en la nube. Los activos en la nube normalmente se facturan en función del uso y deben aprovisionarse y supervisarse cuidadosamente para evitar que la organización pague por partes del servicio que no necesita. La administración de la configuración debe asegurarse de que existen las directivas de supervisión adecuadas para asegurarse de que solo se implementan los recursos necesarios.

Aplicaciones

Las aplicaciones incluyen aplicaciones comerciales instaladas localmente, servicios web y cualquier servicio de aplicaciones implementado en la nube, como Software como servicio (SaaS). El número adecuado de licencias debe mantenerse para todas las aplicaciones comerciales. Una organización debe revisar periódicamente sus necesidades de concesión de licencias. Para las implementaciones en la nube de servicios de software, la administración de configuración debe utilizarse para garantizar que solo el personal que tenga necesidades válidas para el software tenga acceso a él.

Gestión de configuración

Aunque en realidad es un subconjunto de administración de cambios, la administración de la configuración se centra específicamente en sacar el orden del caos que puede ocurrir cuando varios ingenieros y técnicos tienen acceso administrativo a los equipos y dispositivos que hacen que la red funcione. Sigue el mismo proceso básico que se discute en"Procesos de gestión del cambio",más adelante en este capítulo, pero puede tomar aún mayor importancia aquí, teniendo en cuenta el impacto que los cambios conflictivos pueden tener (y en algunos inmediatamente) en una red.

Las siguientes son las funciones de la administración de configuración:

- Informe del estado del procesamiento de cambios.
- Documente las características funcionales y físicas de cada elemento de configuración.
- Realice la captura de información y el control de versiones.
- Controle los cambios en los elementos de configuración y emita versiones de elementos de configuración de la biblioteca de software.

nota

En el contexto de la administración de configuración, una *biblioteca de software* es un área controlada accesible solo para los usuarios aprobados que están restringidos al uso de un procedimiento aprobado. Un *elemento de configuración* (CI) es un subconjunto identificable de forma única del sistema que representa la parte más pequeña que se va a estar sujeta a un procedimiento de control de configuración independiente. Cuando una operación se divide en IA individuales, el proceso se denomina *identificación de configuración.*

Ejemplos de este tipo de cambios son

- Configuración del sistema operativo
- Configuración de software
- Configuración de hardware

Desde una perspectiva CISSP, la mayor contribución de los controles de administración de configuración es garantizar que los cambios en el sistema no disminuyan involuntariamente la seguridad. Debido a esto, todos los cambios deben documentarse, y todos los diagramas de red, tanto lógicos como físicos, *deben* actualizarse constantemente y de forma coherente para reflejar con precisión el estado de cada configuración *ahora* y no como lo era hace dos años. La comprobación de que se están siguiendo todas las directivas de administración de configuración debe ser un proceso continuo.

En muchos casos es beneficioso formar una placa de control de configuración. Las tareas de la placa de control de configuración pueden incluir

- Asegurarse de que los cambios realizados se aprueban, prueban, documentan e implementan correctamente.
- Reunión periódica para discutir los informes de contabilidad de estado de configuración.
- Mantener la responsabilidad de garantizar que los cambios realizados no pongan en peligro la solidez del sistema de verificación.

En resumen, los componentes de la administración de la configuración son

- Control de configuración
- Contabilidad de estado de configuración
- Auditoría de configuración

CONCEPTOS DE OPERACIONES DE SEGURIDAD

A lo largo de este libro, ha visto referencias hechas a políticas y principios que pueden guiar todas las operaciones de seguridad. En esta sección, revisamos algunos conceptos más completamente que ya han sido tocados e introducimos algunos nuevos problemas relacionados con el mantenimiento de las operaciones de seguridad.

Necesidad de saber / privilegio mínimo

Con respecto a permitir el acceso a los recursos y asignar derechos para realizar operaciones, aplique siempre el concepto de privilegio mínimo (también llamado necesidad de saber). En el contexto del acceso a los recursos, esto significa que el nivel predeterminado de acceso no debe tener *acceso*. Dé a los usuarios acceso solamente a los recursos necesarios para hacer su trabajo, y que el acceso debe requerir la implementación manual después de que un supervisor verifique el requisito.

El control de acceso discrecional (DAC) y el control de acceso basado en roles (RBAC) son ejemplos de sistemas basados en la necesidad de saber de un usuario. Para garantizar el menor privilegio se requiere que se identifique el trabajo del usuario y que cada usuario reciba la autorización más baja necesaria para sus tareas. Otro ejemplo es la implementación de vistas en una base de datos. La necesidad de saber requiere que el operador tenga el mínimo conocimiento del sistema necesario para realizar su tarea.

Administración de cuentas, grupos y roles

Los dispositivos, equipos y aplicaciones implementan cuentas y roles de usuario y grupo para permitir o denegar el acceso. Se crean cuentas de usuario para cada usuario que necesita acceso. Las cuentas de grupo se usan para configurar permisos en los recursos. Las cuentas de usuario se agregan a las cuentas de grupo adecuadas para heredar los permisos concedidos a ese grupo. Las cuentas de usuario también se pueden asignar a roles. Las aplicaciones utilizan los roles con mayor frecuencia.

Los profesionales de la seguridad deben comprender las siguientes cuentas:

- **Cuentas de administrador raíz o integradas:** Estas son las cuentas más poderosas del sistema. Las cuentas raíz se utilizan en sistemas basados en Linux, mientras que las cuentas de administrador se utilizan en sistemas basados en Windows. Es mejor deshabilitar una cuenta de este tipo después de haber creado otra cuenta con los mismos privilegios, porque la mayoría de estos nombres de cuenta son bien conocidos y pueden ser utilizados por los atacantes. Si decide conservar estas cuentas, la mayoría de los proveedores sugieren que cambie el nombre de la cuenta y le proporcione una contraseña compleja. Las cuentas raíz o de administrador solo deben

utilizarse al realizar tareas administrativas y el uso de estas cuentas siempre debe auditarse.

- **Cuentas de servicio:** Estas cuentas se utilizan para ejecutar servicios y aplicaciones del sistema. Por lo tanto, los profesionales de seguridad pueden limitar el acceso de la cuenta de servicio al sistema. Investigue siempre las cuentas de usuario predeterminadas que se usan. Asegúrese de cambiar las contraseñas de estas cuentas de forma regular. El uso de estas cuentas siempre debe auditarse.

- **Cuentas de administrador regulares:** Estas cuentas de administrador se crean y asignan solo a una sola persona. Cualquier usuario que tenga una cuenta administrativa también debe tener una cuenta de usuario normal/estándar para usar para las operaciones diarias normales. Las cuentas administrativas solo deben utilizarse al realizar tareas de nivel administrativo, y el uso de estas cuentas siempre debe auditarse.

- **Cuentas de usuario de energía:** Estas cuentas tienen más privilegios y permisos que las cuentas de usuario normales. Estas cuentas deben revisarse regularmente para asegurarse de que solo los usuarios que necesitan los permisos de nivel superior tienen estas cuentas. La mayoría de los sistemas operativos modernos limitan las capacidades de los usuarios avanzados o incluso eliminan este tipo de cuenta por completo.

- **Cuentas de usuario normales/estándar:** Estas son las cuentas que los usuarios utilizan mientras realizan sus tareas laborales diarias normales. Estos relatos deben seguir estrictamente el principio de privilegio mínimo.

Separación de deberes y responsabilidades

El concepto de separación de funciones establece que las operaciones sensibles se dividan entre múltiples usuarios para que ningún usuario tenga los derechos y el acceso para llevar a cabo la operación por sí solo. La separación de funciones y responsabilidades es valiosa para disuadir el fraude al asegurar que ninguna persona puede comprometer un sistema. Se considera un control administrativo *preventivo*. Un ejemplo sería una persona que inicia una solicitud de pago y otra autoriza ese mismo pago. Esto también se conoce a veces como *control dual*.

Gestión de cuentas privilege

Los profesionales de la seguridad deben asegurarse de que las organizaciones establezcan los procedimientos de administración de ciclo de vida de cuentas, grupos y roles adecuados para garantizar que se crean, administran y eliminan correctamente. El ciclo de vida de aprovisionamiento se cubre con más detalle en el capítulo 5,"Gestión de identidades y accesos (IAM)"."

Inevitablemente, algunos usuarios, especialmente los supervisores o aquellos en el departamento de soporte de TI, requerirán derechos y privilegios especiales que otros usuarios no poseen. Por ejemplo, es posible que sea

necesario que un conjunto de usuarios que trabajan en el servicio de ayuda necesiten poder restablecer contraseñas o quizás realizar cambios en las cuentas de usuario. Este tipo de derechos conllevan la responsabilidad de ejercer los derechos de manera responsable y ética.

Aunque en un mundo perfecto nos gustaría asumir que podemos esperar esto de todos los usuarios, en el mundo real sabemos que esto no siempre es cierto. Por lo tanto, una de las cosas a supervisar es el uso de estos privilegios y cuentas con privilegios. Aunque deberíamos preocuparnos por la cantidad de supervisión realizada y la cantidad de datos producidos por esta supervisión, no se debe sacrificar el registro del ejercicio de privilegios especiales o el uso de cuentas con privilegios, incluso si significa guardar regularmente los datos como un archivo de registro y borrar el sistema de recopilación de eventos.

Rotación de empleo y vacaciones obligatorias

Desde una perspectiva de seguridad, la rotación del trabajo se refiere a la capacitación de varios usuarios para realizar las tareas de un puesto para ayudar a prevenir el fraude por parte de cualquier empleado individual. La idea es que al hacer que varias personas se familiaricen con las funciones legítimas del puesto, mayor será la probabilidad de que las actividades inusuales de cualquier persona se noten. Esto se utiliza a menudo junto con *las vacaciones obligatorias,*en las que todos los usuarios están obligados a tomarse un tiempo libre, lo que permite a otro llenar su puesto mientras se ha ido, lo que mejora la oportunidad de descubrir actividades inusuales. Más allá de los aspectos de seguridad de la rotación de trabajos, los beneficios adicionales incluyen

- Respaldo capacitado en caso de emergencias
- Protección contra el fraude
- Formación cruzada de los empleados

La rotación de funciones, la separación de funciones y las vacaciones obligatorias son todos controles administrativos.

Control de dos personas

Un control de dos personas, también conocido como regla de dos hombres, ocurre cuando ciertos accesos y acciones requieren la presencia de dos personas autorizadas en todo momento. Ejemplos comunes de esto son el requisito de que dos personas firmen cheques por una cierta cantidad en dólares o que dos personas estén presentes para realizar una determinada actividad, como abrir una caja fuerte.

Procedimientos de información sensibles

El control de acceso y su uso para evitar el acceso no autorizado a datos confidenciales son importantes para la seguridad de la organización. De ello se deduce que el manejo seguro de la información confidencial es fundamental.

Aunque tendemos a pensar en términos de la información de la empresa, también es fundamental que la empresa proteja la información privada de sus clientes y empleados también. Una filtración de información personal de usuarios y clientes causa una vergüenza mínima para la compañía y posiblemente multas y demandas.

Independientemente de si el objetivo es proteger los datos de la empresa o los datos personales, la clave es aplicar los principios de control de acceso a ambos conjuntos de datos. Al examinar el acceso a los procedimientos y políticas de control de acceso, deben responderse las siguientes preguntas:

- ¿Están disponibles los datos para el usuario que no es necesario para su trabajo?
- ¿Demasiados usuarios tienen acceso a datos confidenciales?

Retención de registros

El control de acceso adecuado no es posible sin auditoría. Esto nos permite realizar un seguimiento de las actividades y descubrir problemas antes de que se realicen plenamente. Dado que esto a veces puede conducir a una montaña de datos para analizar, solo supervisar las actividades más sensibles y conservar y revisar todos los registros. Además, en muchos casos, la ley o la regulación exigen a las empresas que mantengan registros de determinados datos.

La mayoría de los sistemas de auditoría permiten la configuración de opciones de retención de datos. En algunos casos, la operación predeterminada consiste en empezar a escribir sobre los registros anteriores del registro cuando el tamaño máximo del registro está lleno. La limpieza y el guardado regulares del registro pueden impedir que esto suceda y evitar la pérdida de eventos importantes. En los casos de datos extremadamente confidenciales, es aconsejable tener un servidor apagado cuando un registro de seguridad está lleno y no puede registrar más eventos.

Ciclo de vida de la información

En las operaciones de seguridad, los profesionales de la seguridad deben comprender el ciclo de vida de la información, que incluye la creación/recepción, distribución, uso, mantenimiento y eliminación de información. Una vez recopilada la información, debe clasificarse para garantizar que solo el personal autorizado pueda acceder a la información.

> **nota**
>
> Para obtener más información sobre el ciclo de vida de la información, consulte el Capítulo 2,"Seguridad de activos."

Acuerdos de nivel de servicio

Los acuerdos de nivel de servicio (SLA) son acuerdos sobre la capacidad del sistema de soporte para responder a problemas dentro de un cierto plazo mientras se proporciona un nivel de servicio acordado. Pueden ser internos entre departamentos o externos a un proveedor de servicios. Al acordar la rapidez con la que se abordan diversos problemas, se introduce cierta previsibilidad en la respuesta a los problemas, que en última instancia apoya el mantenimiento del acceso a los recursos.

El SLA debe contener una descripción de los servicios que se proporcionarán y los niveles de servicio y métricas esperados que el cliente puede esperar. También incluye los deberes y responsabilidades de cada parte del SLA. Enumera los detalles del servicio, las exclusiones, los niveles de servicio, los procedimientos de escalado y el costo. Debe incluir una cláusula relativa al pago a los clientes resultante de una infracción del SLA. Si bien los SLA pueden ser transferibles, no son transferibles por ley. Las métricas que se deben medir incluyen la disponibilidad del servicio, los niveles de servicio, las tasas de defectos, la calidad técnica y la seguridad. Los SLA deben revisarse periódicamente para asegurarse de que las necesidades empresariales, el entorno técnico o las cargas de trabajo no han cambiado. Además, las métricas, las herramientas de medición y los procesos deben revisarse para ver si han mejorado.

PROTECCIÓN DE RECURSOS

Los recursos empresariales incluyen tanto activos que podemos ver y tocar (tangibles), como computadoras e impresoras, y activos que no podemos ver y tocar (intangibles), como secretos comerciales y procesos. Aunque normalmente pensamos en la protección de los recursos como la prevención de la corrupción de los recursos digitales y como la prevención de daños a los recursos físicos, este concepto también incluye mantener la disponibilidad de esos recursos. En esta sección, discutimos ambos aspectos de la protección de recursos.

Protección de activos tangibles e intangibles

En algunos casos, entre los activos más valiosos de una empresa se encuentran los intangibles, como recetas secretas, fórmulas y secretos comerciales. En otros casos, el valor de la empresa se deriva de sus activos físicos como instalaciones, equipos y el talento de su gente. Todos se consideran recursos y deben incluirse en un plan integral de protección de recursos. En esta sección, se exploran algunas preocupaciones específicas con estos diversos tipos de recursos.

Instalaciones

Por lo general, el mayor activo tangible que tiene una organización es el edificio en el que opera y los terrenos circundantes. La seguridad física se cubre más adelante en este capítulo, pero cabe destacar que las pruebas de

vulnerabilidad (debatidas más plenamente en el capítulo 6)deberían incluir los controles de seguridad de la propia instalación. Algunos ejemplos de pruebas de vulnerabilidad en lo que se refiere a las instalaciones incluyen

- ¿Las puertas se cierran automáticamente y suena una alarma si se mantienen abiertas demasiado tiempo?
- ¿Son suficientes y operativos los mecanismos de protección de las áreas sensibles, como las salas de servidores y los armarios de cableado?
- ¿Funciona el sistema de extinción de incendios?
- ¿Se trituran documentos sensibles en lugar de ser arrojados al basurero?

Más allá de los problemas de acceso, los principales sistemas que se necesitan para garantizar que las operaciones no se interrumpan incluyen detección/supresión de incendios, HVAC (incluidos controles de temperatura y humedad), sistemas de agua y alcantarillado, energía de energía/respaldo, equipos de comunicaciones y detección de intrusiones.

hardware

Otro de los activos más tangibles que deben protegerse es todo el hardware que hace que la red funcione. Esto incluye no sólo los ordenadores e impresoras con los que los usuarios entran directamente en contacto, sino también los dispositivos de infraestructura que nunca ven, como enrutadores, conmutadores y dispositivos de firewall. El mantenimiento del acceso a estos dispositivos críticos desde un punto de vista de disponibilidad se cubre más adelante en las secciones"Redundancia y tolerancia a errores"y"Sistemas de copia de seguridad y recuperación."

Desde el punto de vista de la administración, estos dispositivos normalmente se administran de forma remota. Se debe tener especial cuidado para salvaguardar el acceso a estas características de administración, así como para proteger los datos y comandos que pasan a través de la red a estos dispositivos. Algunas directrices específicas incluyen

- Cambie todas las contraseñas de administrador predeterminadas en los dispositivos.
- Limite el número de usuarios que tienen acceso remoto a estos dispositivos.
- En lugar de Telnet (que envía comandos en cleartext), utilice una herramienta de línea de comandos cifrada como Secure Shell (SSH).
- Gestione sistemas críticos localmente.
- Limite el acceso físico a estos dispositivos.

software

Los activos de software incluyen cualquier aplicación de propiedad, scripts o archivos por lotes que se hayan desarrollado internamente y que sean críticos para el funcionamiento de la organización. Las prácticas seguras de codificación y desarrollo pueden ayudar a prevenir debilidades en estos sistemas. También se debe prestar atención a la prevención del robo de estos activos también.

Además, el seguimiento de cerca el uso de aplicaciones y sistemas comerciales en la empresa puede evitar el incumplimiento involuntario de los acuerdos de concesión de licencias. Una de las ventajas de dar sólo a los usuarios las aplicaciones que requieren para hacer su trabajo es que limita el número de usuarios que tienen una aplicación, ayudando a evitar el agotamiento de las licencias para el software.

> **nota**
>
> La seguridad de desarrollo de software se discute en detalle en el Capítulo 8,"Seguridad de desarrollo de software."

Activos de información

Los activos de información son el último tipo de activo que debe discutirse, pero de ninguna manera son los menos importantes. El objetivo *principal* de la seguridad de las operaciones es salvaguardar los activos de información que residen en el sistema. Estos activos incluyen recetas, procesos, secretos comerciales, planes de productos y cualquier otro tipo de información que permita a la empresa mantener la competitividad dentro de su industria. Los principios de clasificación de datos y control de acceso se aplican de forma más crítica a estos activos. En algunos casos, el valor en dólares de estos activos podría ser difícil de determinar, aunque podría quedar claro para todos los involucrados que el activo es crítico. Por ejemplo, la fórmula secreta para Coca-Cola ha estado estrechamente protegida durante muchos años debido a su valor para la compañía.

Gestión de activos

En el proceso de gestión de estos activos, se deben abordar varias cuestiones. Ciertamente, el acceso al activo debe estar estrechamente controlado para evitar su supresión, robo o corrupción (en el caso de los activos digitales) y de daños físicos (en el caso de los activos físicos). Además, el activo debe permanecer disponible cuando sea necesario. En esta sección se tratan los métodos para garantizar la disponibilidad, la autorización y la integridad.

Redundancia y tolerancia a fallos

Una forma de proporcionar acceso ininterrumpido a los activos de información es mediante redundancia y tolerancia a errores. Redundancia hace referencia a proporcionar varias instancias de un componente físico o

lógico de modo que un segundo componente esté disponible si se produce un error en el primero. La tolerancia a errores es un concepto más amplio que incluye redundancia, pero hace referencia a cualquier proceso que permita a un sistema seguir poniendo a disposición activos de información en caso de error.

En algunos casos, la redundancia se aplica en la capa física, como la redundancia de red proporcionada por una estructura básica dual en un entorno de red local o mediante el uso de varias tarjetas de red en un servidor crítico. En otros casos, la redundancia se aplica lógicamente como cuando un router conoce las trayectorias múltiples a un destino en caso de que se produzca un error.

Las contramedidas de tolerancia a fallos están diseñadas para combatir las amenazas a la fiabilidad del diseño. Aunque la tolerancia a errores puede incluir redundancia, también hace referencia a sistemas como redundante matriz de discos independientes (RAID) en los que los datos se escriben en varios discos de tal manera que un disco puede fallar y los datos se pueden poner rápidamente a disposición de los discos restantes de la matriz sin recurrir a una cinta de copia de seguridad. Esté familiarizado con una serie de tipos RAID porque no todos proporcionan tolerancia a errores. Independientemente de la técnica empleada para que la tolerancia a fallos funcione, un sistema debe ser capaz de detectar y corregir el fallo.

Sistemas de copia de seguridad y recuperación

Aunque a lo largo de este capítulo se encuentra una cobertura integral de los sistemas de backup y recuperación, es importante destacar aquí el papel de las operaciones en la realización de esas actividades. Una vez diseñado el calendario de copia de seguridad, habrá tareas diarias asociadas a la realización del plan. Una de las partes más importantes de este sistema es un proceso de prueba continuo para garantizar que todas las copias de seguridad se pueden usar en caso de que se requiera una recuperación. El momento de descubrir que una copia de seguridad no se realizó correctamente es durante las pruebas y no durante una recuperación en vivo.

Gestión de identidad y acceso

Desde el punto de vista de las operaciones, es importante darse cuenta de que la administración de estas cosas es un proceso continuo que podría requerir la creación de cuentas, la eliminación de cuentas, la creación y la creación de grupos y la administración de los permisos asociados a todos estos conceptos. Es esencial garantizar que los derechos para realizar estas acciones estén estrechamente controlados y que se establezca un proceso formal para eliminar permisos cuando ya no sean necesarios y deshabilitar las cuentas que ya no son necesarias.

Otra área en la que centrarse es el control del uso de cuentas o cuentas con privilegios que tienen derechos y permisos que superan los de una cuenta de usuario normal. Aunque esto obviamente se aplica a las cuentas de

administrador, raíz o supervisor integradas (que en algunos sistemas operativos se denominan cuentas raíz) que tienen permisos vastos, también se aplica a cualquier cuenta que confiere privilegios especiales al usuario.

Además, mantenga el mismo estricto control sobre los numerosos grupos integrados que existen en Windows para conceder derechos especiales a los miembros del grupo. Al usar estos grupos, anote los privilegios que tienen los grupos predeterminados que no sean necesarios para sus propósitos. Es posible que desee quitar algunos de los privilegios de los grupos predeterminados para admitir el concepto de privilegios mínimos. Puede obtener más información sobre la identidad y la gestión de accesos en el Capítulo 5.

Gestión de medios

La administración de medios es una parte importante de la seguridad de las operaciones porque los medios son donde se almacenan los datos. La administración de medios incluye RAID, SAN, NAS y HSM.

incursión

Matriz redundante de discos independientes (RAID) hace referencia a un sistema mediante el cual se utilizan varios discos duros para proporcionar un aumento del rendimiento o tolerancia a errores para los datos. Cuando hablamos de tolerancia a errores en RAID, nos referimos a mantener el acceso a los datos incluso en un error de unidad sin restaurar los datos de los medios de copia de seguridad. A continuación se presentan los tipos de RAID con los que debe estar familiarizado.

RAID 0, también denominado seccionamiento de disco, escribe los datos en varias unidades. Aunque mejora el rendimiento, no proporciona tolerancia a errores. La Figura 7-3 representa RAID 0.

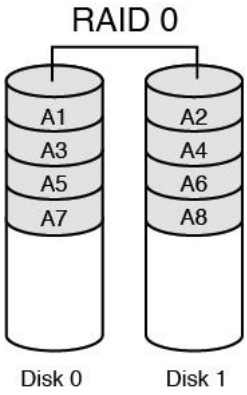

Figura 7-3 RAID 0

RAID 1, también denominada creación de reflejo del disco, utiliza dos discos y escribe una copia de los datos en ambos discos, proporcionando tolerancia a errores en el caso de un único error de unidad. La Figura 7-4 representa RAID 1.

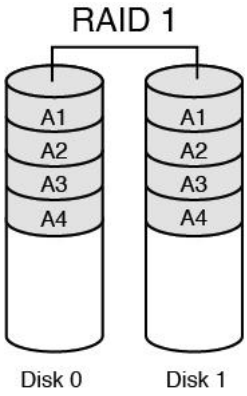

Figura 7-4 RAID 1

*RAID 3,*que requiere al menos tres unidades, también requiere que los datos se escriban en todas las unidades, como el rayado y, a continuación, se escriba *información de paridad* en una sola unidad dedicada. La información de paridad se utiliza para regenerar los datos en caso de un único error de unidad. La caída es que la unidad de paridad es un único punto de error si va mal. La Figura 7-5 representa RAID 3.

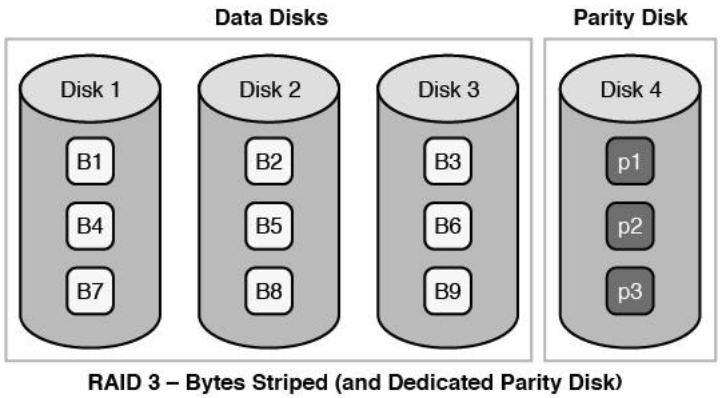

Figure 7-5 RAID 3

*RAID 5,*que requiere al menos tres unidades, también requiere que los datos se escriban en todas las unidades, como el rayado y, a continuación, también se escriba información de paridad en todas las unidades. La información de paridad se utiliza de la misma manera que en RAID 3, pero no se almacena en una sola unidad, por lo que no hay un único punto de error para los datos de paridad. Con el nivel RAID de hardware 5, las unidades de repuesto que reemplazan a las unidades con errores suelen ser intercambiables en caliente, lo que significa que se pueden reemplazar en el servidor mientras se está ejecutando. La Figura 7-6 representa RAID 5.

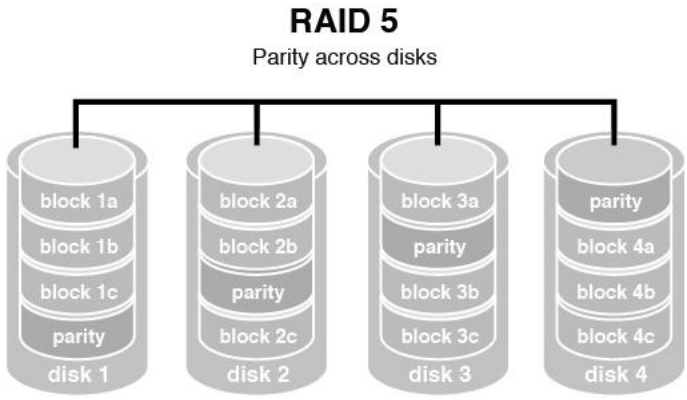

Figure 7-6 RAID 5

*RAID 10,*que requiere al menos cuatro unidades, es una combinación de RAID 0 y RAID 1. En primer lugar, se crea un volumen RAID 1 reflejando dos unidades juntas. A continuación, se crea un conjunto de rayas RAID 0 en cada par reflejado. La Figura 7-7 representa RAID 10.

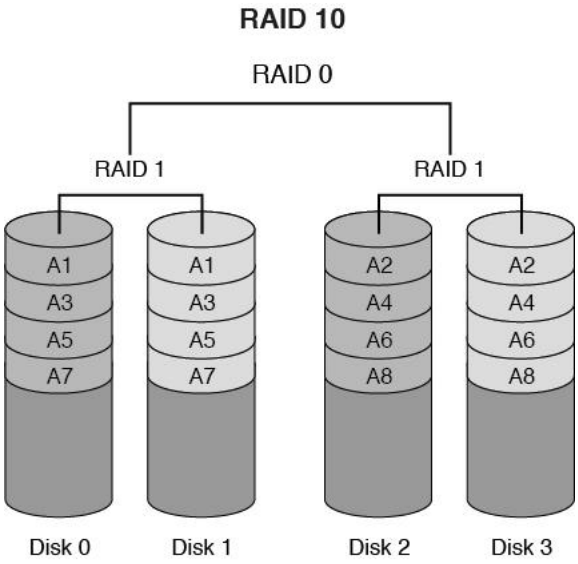

Figure 7-7 RAID 10

Aunque RAID se puede implementar con software o con hardware, ciertos tipos de RAID son más rápidos cuando se implementan con hardware. Cuando se utiliza RAID de software, es una función del sistema operativo. Tanto RAID 3 como 5 son ejemplos de tipos RAID que son más rápidos cuando se implementan con hardware. Sin embargo, el seccionado o espejado simple (RAID 0 y 1) tienden a funcionar bien en el software porque no utilizan las unidades de paridad de nivel de hardware. La Tabla 7-1 resume los tipos RAID.

Tabla 7-1 Niveles RAID

Nivel RAID	Número mínimo de unidades	descripción	Fortalezas	Debilidades
RAID 0	2	Rayado de datos sin redundancia	Mayor rendimiento	Sin protección de datos; una unidad falla, todos los datos se pierden
RAID 1	2	Duplicación de disco	Muy alto rendimiento; protección de datos muy alta; penalización muy mínima en el rendimiento de escritura	Gastos generales de alto costo de redundancia; debido a que todos los datos se duplican, se requiere el doble de capacidad de almacenamiento
RAID 3	3	Rayado de datos a nivel de byte con unidad de paridad dedicada	Excelente rendimiento para solicitudes de datos grandes y secuenciales	No es adecuado para aplicaciones de red orientadas a transacciones; unidad de paridad única no admite múltiples solicitudes simultáneas de lectura y escritura

Nivel RAID	Número mínimo de unidades	descripción	Fortalezas	Debilidades
RAID 5	3	Seccionado de datos a nivel de bloque con paridad distribuida	Mejor costo/rendimiento para redes orientadas a transacciones; muy alto rendimiento, muy alta protección de datos; soporta múltiples lecturas y escrituras simultáneas; también se puede optimizar para solicitudes grandes y secuenciales	El rendimiento de escritura es más lento que RAID 0 o RAID 1
RAID 10	4	Duplicación de disco con rayado	La misma tolerancia a errores que RAID 1; la misma sobrecarga que con la duplicación; proporciona altas tasas de E/S; puede sufrir múltiples fallas simultáneas en la unidad	Muy caro; todas las unidades deben moverse en paralelo a la pista correcta, lo que reduce el rendimiento sostenido; escalabilidad muy limitada a un costo muy alto

San

Las redes de área de almacenamiento (SAN) se componen de dispositivos de almacenamiento de alta capacidad conectados por una red privada de alta velocidad (independiente de la LAN) mediante conmutadores específicos del almacenamiento. Esta arquitectura de información de almacenamiento aborda la recopilación de datos, la administración de datos y el uso de datos.

Nas

El almacenamiento conectado a la red (NAS) cumple la misma función que SAN, pero los clientes acceden al almacenamiento de una manera diferente. En un NAS, casi cualquier máquina que pueda conectarse a la LAN (o está interconectada a la LAN a través de una WAN) puede utilizar protocolos como NFS, CIFS o HTTP para conectarse a un NAS y compartir archivos. En una SAN, solo los dispositivos que pueden utilizar la red SCSI fibre channel pueden acceder a los datos, por lo que normalmente se realiza a través de un servidor que tiene esta capacidad. La Figura 7-8 muestra una comparación de los dos sistemas.

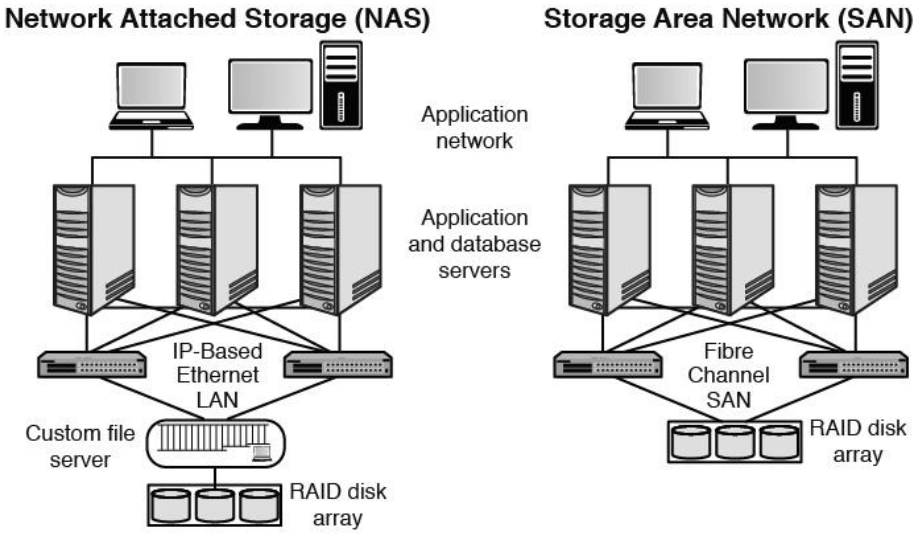

Figura 7-8 NAS y SAN

Hsm

Un sistema jerárquico de gestión del almacenamiento de información (HSM) es un tipo de sistema de gestión de backup que proporciona una copia de seguridad en línea continua mediante el uso de "jukeboxes" ópticos o de cinta. Funciona moviendo automáticamente datos entre medios de almacenamiento de alto costo y bajo costo a medida que los datos envejecen. Cuando se requiere disponibilidad continua (procesamiento las 24 horas del día), HSM proporciona una buena alternativa a las copias de seguridad en cinta. También se esfuerza por utilizar los medios adecuados para el escenario. Por ejemplo, a veces se utiliza un disco óptico regrabable y borrable (CDR/W) para copias de seguridad que requieren almacenamiento de poco tiempo para datos modificables, pero requieren un acceso a archivos más rápido que la cinta.

> **nota**
>
> No confundas el acrónimo HSM. HSM también puede referirse al módulo de secur-ity de hardware, que es un dispositivo que administra y protege las claves digitales para una autenticación segura.

Historia de los medios

Mantenga con precisión los registros de la biblioteca multimedia para realizar un seguimiento del historial de los medios. Esto es importante en el hecho de que todos los tipos de medios tienen un número máximo de veces que se pueden utilizar de forma segura. Un bibliotecario de medios debe guardar un registro. Este registro debe realizar un seguimiento de todos los medios (copia de seguridad y otros tipos, como discos de instalación del sistema operativo y memoria USB). Con respecto a los medios de copia de seguridad, utilice las siguientes directrices:

- Realice un seguimiento de todas las instancias de acceso a los medios.
- Realice un seguimiento del número y la ubicación de las copias de seguridad.
- Realice un seguimiento de la edad de los medios de comunicación para evitar la pérdida de datos a través de la degeneración de los medios de comunicación.
- Inventariar los medios regularmente.

Etiquetado y almacenamiento de medios

Etiquete claramente todas las formas de medios de almacenamiento (cintas, unidades ópticas, unidades USB, etc.) y guárdelos de forma segura. Algunas directrices en el ámbito del control de los medios de comunicación son

- Marque con precisión y prontitud todos los medios de almacenamiento de datos.
- Garantizar el almacenamiento ambiental adecuado de los medios.
- Garantizar el manejo seguro y limpio de los medios.
- Registre los medios de datos para proporcionar un control de inventario físico.

El entorno donde se almacenarán los medios también es importante. Por ejemplo, el daño comienza a producirse en medios magnéticos por encima de los 100 grados. El *Libro Verde del Bosque* es un libro de la Serie Rainbow que define el manejo seguro de la memoria sensible o clasificada del sistema de información automatizada y los medios de almacenamiento secundarios, como degaussers, cintas magnéticas, discos duros y tarjetas. La Serie Arco Iris se discute con más detalle en el Capítulo 3.

Desinfectar y deshacerse de los medios de comunicación

Durante la eliminación de medios, debe asegurarse de que no quedan datos en los medios. El medio más fiable y seguro de eliminar datos de medios de almacenamiento magnético, como un casete de cinta magnética, es a través de la desgaussing, que expone los medios a un potente campo magnético alterno.

Elimina los datos escritos previamente, dejando los medios en un estado magnéticamente aleatorio (en blanco). Algunos otros términos y conceptos de eliminación con los que usted debe estar familiarizado son

- **Purga de datos:** Usar un método como degaussing para que los datos antiguos no estén disponibles incluso con los forenses. Purgar hace que la información sea irrecuperable contra ataques de laboratorio (forenses).

- **Compensación de datos:** Representa la información irrecuperable por un teclado. Este ataque extrae información de los medios de almacenamiento de datos mediante la ejecución de utilidades de software, pulsaciones de teclas u otros recursos del sistema ejecutados desde un teclado.

- **Remanencia:** Cualquier dato que quede después de que los medios hayan sido borrados.

Gestión de redes y recursos

Aunque las operaciones de seguridad se centran en proporcionar confidencialidad e integridad de los datos, la disponibilidad de los datos también es uno de sus objetivos. Esto significa diseñar y mantener procesos y sistemas que mantienen la disponibilidad de recursos a pesar de fallos de hardware o software en el entorno. Se dispone de los siguientes principios y conceptos para ayudar a mantener el acceso a los recursos:

- **Hardware redundante:** Los errores de los componentes físicos, como los discos duros y las tarjetas de red, pueden interrumpir el acceso a los recursos. Proporcionar instancias redundantes de estos componentes puede ayudar a garantizar una vuelta más rápida al acceso. En algunos casos, cambiar un componente puede requerir una intervención manual, pero en muchos casos estos elementos son intercambiables en caliente (se pueden cambiar con el dispositivo en funcionamiento), en cuyo caso podría producirse una reducción momentánea del rendimiento en lugar de una interrupción completa del acceso.

- **Tecnologías tolerantes a fallos:** Llevar la idea de redundancia al siguiente nivel son tecnologías basadas en múltiples sistemas informáticos que trabajan juntos para proporcionar acceso ininterrumpido incluso en caso de fallo de uno de los sistemas. La agrupación en clústeres de servidores y la informática de red son dos grandes ejemplos de este enfoque.

- **Acuerdos de nivel de servicio (SLA):** Los SLA son acuerdos sobre la capacidad del sistema de soporte para responder a los problemas dentro de un cierto plazo mientras se proporciona un nivel de servicio acordado. Pueden ser internos entre departamentos o externos a un proveedor de servicios. Al acordar la rapidez con la que se abordan diversos problemas, se introduce cierta previsibilidad en la respuesta a los problemas, que en última instancia apoya el mantenimiento del acceso a los recursos.

- **MTBF y MTTR:** Aunque los SLA son adecuados para los servicios que se proporcionan, se puede utilizar un enfoque ligeramente diferente para introducir la previsibilidad con respecto a los componentes físicos que se compran. Los proveedores suelen publicar valores para el tiempo medio de un producto entre el error (MTBF), que describe la frecuencia con la que un componente produce un error en promedio. Otra métrica valiosa típicamente proporcionada es el tiempo medio de reparación (MTTR), que describe la cantidad promedio de tiempo que tomará para conseguir el dispositivo fijo y de nuevo en línea.

- **Punto único de error (SPOF):** Aunque en realidad no es una estrategia, vale la pena mencionar que el objetivo final de cualquiera de estos enfoques es evitar un SPOF en un sistema. Todos los componentes y grupos de componentes y dispositivos deben examinarse para detectar cualquier elemento único que pueda interrumpir el acceso a los recursos si se produce un error. Cada SPOF debe mitigarse de alguna manera.

GESTIÓN DE INCIDENTES

La respuesta y la administración de incidentes son vitales para todas las organizaciones para garantizar que se detecten, contengan e investiguen cualquier incidente de seguridad. La respuesta a incidentes es el comienzo de cualquier investigación. Después de que se ha descubierto un incidente, el personal de respuesta a incidentes realiza tareas específicas. Durante toda la respuesta al incidente, el equipo de respuesta a incidentes debe asegurarse de que siguen los procedimientos adecuados para asegurarse de que se conservan las pruebas. La administración de incidentes garantiza que el equipo de respuesta a incidentes administra el incidente y devuelve el servicio a la normalidad lo antes posible después de un incidente.

Como parte de la respuesta a incidentes, los profesionales de seguridad deben comprender la diferencia entre eventos e incidentes (consulte la siguiente sección). El equipo de respuesta a incidentes debe tener los procedimientos de respuesta a incidentes apropiados para asegurarse de que el incidente se maneje, pero los procedimientos no deben obstaculizar ninguna investigación forense que pueda ser necesaria para asegurar que las partes sean consideradas responsables de cualquier acción ilegal. Los profesionales de la seguridad deben comprender las reglas de participación y la autorización y el alcance de cualquier investigación de incidentes.

Evento versus incidente

Con respecto a la respuesta a incidentes, existe una diferencia básica entre eventos e incidentes. Un *evento* es un cambio de estado que se produce. Mientras que los eventos incluyen eventos negativos y positivos, la respuesta a incidentes se centra más en eventos negativos, eventos que se han considerado como que afectan negativamente a la organización. Un *incidente* es una serie de eventos que afectan negativamente a las operaciones y la seguridad de una organización.

Los eventos solo se pueden detectar si una organización ha establecido los mecanismos de auditoría y seguridad adecuados para supervisar la actividad. Puede producirse un único evento negativo. Por ejemplo, el registro de auditoría podría mostrar que se ha producido un intento de inicio de sesión no válido. Por sí mismo, este intento de inicio de sesión no es un problema de seguridad. Sin embargo, si muchos intentos de inicio de sesión no válidos se producen durante un período de unas pocas horas, es posible que la organización esté sufriendo un ataque. El inicio de sesión no válido inicial se considera un evento, pero la serie de intentos de inicio de sesión no válidos durante unas horas sería un incidente, especialmente si se descubre que los intentos de inicio de sesión no válidos se originaron desde la misma dirección IP.

Equipo de respuesta a incidentes e investigaciones de incidentes

Al establecer el equipo de respuesta a incidentes, las organizaciones deben considerar el conocimiento técnico de cada individuo. Los miembros del equipo deben entender la política de seguridad de la organización y tener fuertes habilidades de comunicación. Los Miembros también deben recibir capacitación en respuesta a incidentes e investigaciones.

Cuando se ha producido un incidente, el objetivo principal del equipo es contener el ataque y reparar cualquier daño causado por el incidente. El aislamiento de seguridad de una escena de incidente debe comenzar inmediatamente cuando se descubre el incidente. Deben preservarse las pruebas y notificarse a las autoridades correspondientes.

El equipo de respuesta a incidentes debe tener acceso al plan de respuesta a incidentes. Este plan debe incluir la lista de autoridades para contactar, funciones y responsabilidades de equipo, una lista de contactos internos, procedimientos para asegurar y preservar pruebas, y una lista de expertos en investigación que pueden ser contactados para obtener ayuda. Se debe crear un manual paso a paso que el equipo de respuesta a incidentes debe seguir para asegurarse de que no se omiten los pasos. Una vez que se haya iniciado el proceso de respuesta al incidente, se deben documentar todas las acciones de respuesta a incidentes.

Si el equipo de respuesta a incidentes determina que se ha cometido un delito, se debe contactar inmediatamente a la alta dirección y a las autoridades competentes.

Reglas de participación, autorización y alcance

Una organización debe documentar las reglas de participación, autorización y alcance para el equipo de respuesta a incidentes. Las reglas de contratación definen qué acciones son aceptables e inaceptables si se ha producido un incidente. La autorización y el alcance proporcionan al equipo de respuesta a incidentes la autoridad para llevar a cabo una investigación y con el alcance permitido de cualquier investigación que deben llevar a cabo.

Las reglas de participación actúan como una guía para el equipo de respuesta a incidentes para asegurarse de que no cruzan la línea de la seducción al encierro. El tentamiento ocurre cuando se brinda la oportunidad de acciones ilegales (atrayendo) pero el atacante toma su propia decisión de llevar a cabo la acción, y el encierro significa alentar a alguien a cometer un delito que el individuo podría no haber tenido ninguna intención de cometer. La seducción es legal, pero plantea argumentos éticos y podría no ser admisible en los tribunales. Por el contrario, el encierro es ilegal.

Procedimientos de respuesta a incidentes

Al realizar la respuesta a incidentes, es importante que el equipo de respuesta a incidentes siga los procedimientos de respuesta a incidentes. Dependiendo de dónde mire, es posible que encuentre diferentes pasos o fases incluidos como parte del proceso de respuesta a incidentes.

Para el examen CISSP, debe recordar los siguientes pasos:

1. Detecte el incidente.
2. Responda al incidente.
3. Mitigar los efectos del incidente.
4. Informe del incidente al personal correspondiente.
5. Recuperarse del incidente.
6. Corrija todos los componentes afectados por el incidente para asegurarse de que se han eliminado todos los rastros del incidente.
7. Revise el incidente y documente todos los hallazgos a medida que se aprendan las lecciones.

La investigación real del incidente se produce durante las medidas de respuesta, mitigación, informe y recuperación. Seguir los procesos de investigación forense y digital apropiados durante la investigación puede garantizar que se conserven las pruebas.

El proceso de respuesta a incidentes se muestra en la Figura 7-9.

Figura 7-9 Proceso de respuesta a incidentes

Gestión de respuesta a incidentes

Inevitablemente se producirán eventos de seguridad, y la respuesta a estos eventos dice mucho sobre lo dañinos que serán los eventos para la organización. Las políticas de respuesta a incidentes deben diseñarse

formalmente, comunicarse y seguirse. Deben abordar específicamente los ciberataques contra los sistemas de TI de una organización.

detectar

El primer paso es detectar el incidente. Antes de cualquier investigación de respuesta a incidentes, los profesionales de seguridad deben realizar primero el triaje adecuado para los activos afectados. Esto incluye detectar inicialmente el incidente y determinar cuán grave es el incidente. En algunos casos, durante la fase de triaje, los profesionales de la seguridad pueden determinar que se ha producido un falso positivo, lo que significa que realmente no se produjo un ataque, a pesar de que una alerta indicaba que sí. Si se confirma un ataque, la respuesta al incidente avanzará en acciones de investigación.

Todos los controles de detectives, como la auditoría, discutidos en el Capítulo 1,"Seguridad y Gestión de Riesgos",están diseñados para proporcionar esta capacidad. El peor tipo de incidente es el que pasa desapercibido.

responder

La respuesta al incidente debe ser adecuada para el tipo de incidente. Los ataques de denegación de servicio (DoS) contra el servidor web requerirían una respuesta más rápida y diferente que un ratón que falta en la sala de servidores. Establezca respuestas estándar y tiempos de respuesta con anticipación.

La respuesta implica contener el incidente y anular los activos afectados para reducir el impacto potencial evitando que otros activos se vean afectados. Se pueden utilizar diferentes métodos, dependiendo de la categoría del ataque, el activo afectado y la criticidad de datos o el riesgo de infección.

Después de que un ataque esté contenido o aislado, los analistas deben trabajar para examinar y analizar la causa del incidente. Esto incluye determinar dónde se originó el incidente. Los profesionales de la seguridad deben utilizar la experiencia y la formación formal para sacar las conclusiones apropiadas sobre el incidente. Una vez determinada la causa raíz, los profesionales de seguridad deben seguir las directivas de control de incidentes que la organización tiene en su lugar.

mitigar

La mitigación incluye limitar el alcance de lo que el ataque podría hacer a los activos de la organización. Si se ha producido un daño o el incidente puede ampliarse y afectar a otros activos, las técnicas de mitigación adecuadas garantizan que el incidente esté contenido dentro de un cierto ámbito de activos. Las opciones de mitigación varían según el tipo de ataque que se haya producido. Los profesionales de la seguridad deben desarrollar procedimientos de antemano que detallen cómo mitigar adecuadamente los ataques que se producen contra activos organizativos. La preparación de estos

procedimientos de mitigación de antemano garantiza que sean exhaustivos y da al personal la oportunidad de probar los procedimientos.

informe

Todos los incidentes deben ser reportados dentro de un plazo que refleje la gravedad del incidente. En muchos casos, es útil establecer una lista de tipos de incidentes y la persona con la que ponerse en contacto cuando se produce ese tipo de incidente. Ejercer la atención al detalle en esta etapa temprana mientras la información sensible al tiempo todavía está disponible es fundamental.

recuperar

La recuperación implica una reacción diseñada para hacer que la red o el sistema que se ve afectado vuelva a funcionar; incluye la reparación de los activos afectados y la prevención de incidentes similares en el futuro. Exactamente lo que significa la recuperación depende de las circunstancias y las medidas de recuperación disponibles. Por ejemplo, si existen medidas de tolerancia a errores, la recuperación podría consistir simplemente en permitir que un servidor de un clúster conmute por error a otro. En otros casos, la recuperación podría significar restaurar el servidor desde una copia de seguridad reciente. El objetivo principal de este paso es hacer que todos los recursos estén disponibles de nuevo. Retrase la puesta en funcionamiento de cualquier activo hasta que esté al menos protegido del incidente que se produjo. Pruebe a fondo los activos en busca de vulnerabilidades y debilidades antes de reintroducirlos en producción.

Remediar

Este paso implica eliminar cualquier peligro residual o daño a la red que todavía pueda existir. Por ejemplo, en el caso de un brote de virus, podría significar escanear todos los sistemas para erradicar cualquier máquina afectada adicional. Estas medidas están diseñadas para realizar una mitigación más detallada cuando el tiempo lo permite.

Lecciones aprendidas y revisión

Por último, revise cada incidente para descubrir lo que se puede aprender de él. Es posible que se res pidan cambios en los procedimientos. Comparta las lecciones aprendidas con todo el personal que pueda volver a encontrarse con este tipo de incidentes. La documentación completa y el análisis son el objetivo de este paso.

DETECTIVE Y MEDIDAS PREVENTIVAS

Como probablemente ya se ha reunido, una amplia variedad de amenazas a la seguridad se enfrentan a los encargados de proteger los activos de una

organización. Afortunadamente, una amplia variedad de herramientas está disponible para llevar a cabo esta tarea. Esta sección cubre algunas amenazas comunes y enfoques de mitigación.

IDS/IPS

La configuración, configuración y supervisión de cualquier sistema de detección de intrusiones y prevención de intrusiones (IDS/IPS) también son responsabilidades continuas de la seguridad de las operaciones. Muchos de estos sistemas deben actualizarse regularmente con las firmas de ataque que les permiten detectar nuevos tipos de ataques. Los motores de análisis que utilizan también a veces tienen actualizaciones que deben aplicarse.

Además, los archivos de registro de sistemas que están configurados para registrar determinados eventos en lugar de realizar acciones específicas cuando se producen necesitan que esos registros se archiven y analicen periódicamente. Gastar grandes sumas de dinero en software que recopila información y luego ignorar esa información no tiene sentido.

El IDS y el IPS se discuten con más detalle anteriormente en este capítulo y en el capítulo 4.

La respuesta a la intrusión es tan importante como la detección y prevención de intrusiones. La respuesta de intrusión consiste en responder adecuadamente a cualquier intento de intrusión. La mayoría de los sistemas utilizan alarmas y señales para comunicarse con el personal o sistemas adecuados cuando se ha intentado una intrusión. Una organización debe responder a las alertas y señales de manera oportuna.

Cortafuegos

Los firewalls se pueden implementar en varios niveles para permitir o impedir la comunicación en función de una variedad de factores. Si el personal descubre que ciertos tipos de tráfico no deseado están ocurriendo, a menudo es bastante fácil configurar un firewall para evitar ese tipo de tráfico. Los firewalls pueden proteger los límites entre redes, tráfico dentro de una subred o un solo sistema. Asegúrese de mantener los firewalls completamente actualizados según las recomendaciones del proveedor. Los firewalls se discuten más a fondo en el Capítulo 4.

Lista blanca/lista negra

La lista blanca se produce cuando una lista de direcciones de correo electrónico aceptables, direcciones de Internet, sitios web, aplicaciones o algún otro identificador se configura como buenos remitentes o según lo permitido. La lista negra identifica a los remitentes malos. La lista de grises está en algún lugar entre las dos entidades de lista que no se pueden identificar como elementos de la lista blanca o de la lista negra. En el caso de la lista gris, la nueva entidad debe pasar por una serie de pruebas para determinar si se incluirá en la lista blanca o en la lista negra.

La lista blanca, la lista negra y la lista gris se utilizan comúnmente con herramientas de filtrado de spam.

Servicios de seguridad de terceros

Es posible que los profesionales de la seguridad deba confiar en los servicios de seguridad de terceros para encontrar amenazas en la empresa. Algunos servicios de seguridad comunes de terceros incluyen malware / detección de virus y honeypots / honeynets. A menudo es más fácil confiar en una solución desarrollada por un tercero que tratar de desarrollar su propia solución interna. Siempre investigue las características proporcionadas con una solución para determinar si satisface las necesidades de su organización. Compare los diferentes productos disponibles para asegurarse de que la organización compra la mejor solución para sus necesidades.

Sandboxing

El espacio aislado es una técnica de virtualización de software que permite que las aplicaciones y los procesos se ejecuten en un entorno virtual aislado. Las aplicaciones y los procesos en el entorno limitado no son capaces de realizar cambios permanentes en el sistema y sus archivos.

Algunos intentos de malware para retrasar o detener la ejecución de código, lo que permite que el espacio aislado para el tiempo de espera. Un entorno sandbox puede utilizar ganchos y comprobaciones ambientales para detectar malware. Estos métodos no impiden muchos tipos de malware. Por esta razón, los servicios de seguridad de terceros son importantes.

Honeypots/Honeynets

Honeypots son sistemas configurados con seguridad reducida para atraer a los atacantes para que los administradores puedan aprender sobre las técnicas de ataque. En algunos casos, redes enteras llamadas honeynets están configuradas atractivamente para este propósito. Este tipo de enfoques sólo deben ser llevados a cabo por empresas con la habilidad de implementarlos y monitorearlos adecuadamente. Algunos servicios de seguridad de terceros pueden proporcionar esta función para las organizaciones.

Anti-malware/Antivirus

Por último, todas las actualizaciones de antivirus y software anti-malware son responsabilidad de la seguridad de las operaciones. Es importante implementar una solución antivirus/anti-malware integral para toda la empresa.

Niveles de recorte

Los niveles de recorte establecen una línea base para los errores normales del usuario y se registrarán infracciones que superen ese umbral para analizar por qué se produjeron las infracciones. Cuando se utilizan niveles de recorte, un cierto número de apariciones de una actividad puede no generar información,

mientras que la grabación de actividades comienza cuando se supera un determinado nivel.

Los niveles de recorte están acostumbrados a

- Reduzca la cantidad de datos que se evaluarán en los registros de auditoría
- Proporcionar una línea base de errores de usuario anteriores que se registrarán violaciones

> **nota**
>
> Los niveles de recorte también se cubren en el capítulo 5.

Desviaciones de las normas

Uno de los métodos que puede utilizar para identificar los problemas de rendimiento que surgen es mediante el desarrollo de estándares o líneas base para el rendimiento de ciertos sistemas. Una vez establecidos estos puntos de referencia, se pueden identificar desviaciones para las normas. Esto es especialmente útil para identificar ciertos tipos de ataques DoS a medida que ocurren. Más allá del beneficio para la seguridad, también ayuda a identificar sistemas que podrían necesitar mejoras antes de que la situación afecte a la productividad.

Eventos inusuales o inexplicables

En algunos casos se producen eventos que parecen no tener ninguna causa lógica. Eso nunca debe ser aceptado como una respuesta cuando ocurren problemas. Aunque normalmente se centra en poner en marcha los sistemas de nuevo, se deben identificar las causas principales de los problemas. Evite la tentación de implementar una solución rápida (a menudo a expensas de la seguridad). Cuando el tiempo lo permite, el uso de un enfoque metódico para encontrar exactamente por qué ocurrió el evento es mejor, porque inevitablemente el problema volverá si no se ha abordado la causa raíz.

Reinicios no programados

Cuando los sistemas se reinician por sí solos, normalmente es un signo de problemas de hardware de algún tipo. Los reinicios deben grabarse y abordarse. El sobrecalentamiento es la causa de muchos reinicios. A menudo, los reinicios también pueden ser el resultado de un ataque DoS. Tener la supervisión del sistema en su lugar para registrar todos los reinicios del sistema e investigar cualquiera que no haya sido iniciado por un humano o que se haya producido como resultado de una actualización automática.

Divulgación no autorizada

La divulgación no autorizada de información es una gran amenaza para las organizaciones. Incluye la destrucción de información, la interrupción del servicio, el robo de información, la corrupción de la información y la modificación indebida de la información. Las soluciones empresariales deben implementarse para supervisar cualquier posible divulgación de información.

Recuperación de confianza

Cuando una aplicación o sistema operativo sufre un error (bloqueo, congelación, etc.), es importante que el sistema responda de una manera que deje el sistema en un estado seguro o que realice una *recuperación de confianza*. Una recuperación de confianza garantiza que no se infringa la seguridad cuando se produce un bloqueo del sistema u otro error del sistema. Es posible que recuerde del Capítulo 3 que el *Libro Naranja* requiere que un sistema sea capaz de una recuperación de confianza para todos los sistemas clasificados B3 o A1.

Rutas de confianza

Una ruta de acceso de confianza es un canal de comunicación entre el usuario o el programa a través del cual está trabajando y la base de equipos de confianza (TCB). El TCB proporciona los recursos para proteger el canal y evitar que se vea comprometido. Por el contrario, una ruta de comunicación que no está protegida por los mecanismos de seguridad normales del sistema se denomina *canal encubierto*. Dando este paso más allá, si la interfaz ofrecida al usuario está protegida de esta manera, se conoce como un *shell de confianza*.

La seguridad de las operaciones debe garantizar que se validen las rutas de acceso de confianza. Esto ocurre mediante la recopilación de registros, el análisis de registros, los análisis de vulnerabilidades, la administración de revisiones y las comprobaciones de integridad del sistema.

Controles de entrada/salida

El principal impulso del control de entrada/salida es aplicar controles o comprobaciones a la entrada que se permite enviar al sistema. Realizar la validación de entrada en toda la información aceptada en el sistema puede garantizar que es del tipo y formato de datos correctos y que no deja el sistema en un estado inseguro.

Además, se debe garantizar una salida segura del sistema (impresiones, informes, etc.). Toda la información confidencial de salida debe requerir una recepción antes de la versión y tener controles de acceso adecuados aplicados independientemente de su formato.

Endurecimiento del sistema

Otro de los objetivos actuales de la seguridad de las operaciones es garantizar que todos los sistemas se hayan endurecido en la medida en que sea posible y sigan proporcionando funcionalidad. El endurecimiento se puede realizar

tanto a base física como lógica. La seguridad física de los sistemas se cubre en detalle más adelante en este capítulo. Desde una perspectiva lógica

- Elimine aplicaciones innecesarias.
- Deshabilite servicios innecesarios.
- Bloquear puertos no requisados.
- Controle estrictamente la conexión de dispositivos de almacenamiento externos y medios si está permitido en absoluto.

Sistemas de gestión de vulnerabilidades

A lo largo de este libro se ha destacado la importancia de realizar pruebas de vulnerabilidad y penetración. Un sistema de gestión de vulnerabilidades es un software que centraliza y, en cierta medida, automatiza el proceso de supervisión y prueba continua de la red en busca de vulnerabilidades. Estos sistemas pueden analizar la red en busca de vulnerabilidades, denunciarlas y, en muchos casos, solucionar el problema sin intervención humana. Aunque son una herramienta valiosa en la caja de herramientas, estos sistemas, independientemente de lo sofisticados que puedan ser, no pueden ocupar el lugar de las pruebas de vulnerabilidad y penetración realizadas por profesionales capacitados.

GESTIÓN DE PARCHES Y VULNERABILIDADES

La administración de revisiones a menudo se considera como un subconjunto de administración de configuración. *Las revisiones de software* son actualizaciones publicadas por los proveedores que solucionan problemas funcionales o cierran lagunas de seguridad en sistemas operativos, aplicaciones y versiones de firmware que se ejecutan en los dispositivos de red.

Para asegurarse de que todos los dispositivos tienen instalados las revisiones más recientes, implemente un sistema formal para garantizar que todos los sistemas reciban las actualizaciones más recientes *después de* realizar pruebas exhaustivas en un entorno que no sea de producción. Es imposible para el proveedor anticipar todos los impactos posibles que un cambio podría tener en los sistemas críticos para el negocio en la red. La empresa es responsable de garantizar que los parches no afecten negativamente a las operaciones.

El ciclo de vida de gestión de parches incluye los siguientes pasos:

1. **Priorización y programación de parches:** Determine la prioridad de las revisiones y programe las revisiones para la implementación.
2. **Pruebas de parches:** Pruebe las revisiones antes de la implementación para asegurarse de que funcionan correctamente y no causan problemas de

sistema o seguridad.

3. **Instalación de parches:** Instale las revisiones en el entorno en vivo.
4. **Evaluación y auditoría de parches:** Después de implementar las revisiones, asegúrese de que las revisiones funcionan correctamente.

Muchas organizaciones implementan un sistema centralizado de administración de revisiones para garantizar que las revisiones se implementen de manera oportuna. Con este sistema, los administradores pueden probar y revisar todas las revisiones antes de implementarlas en los sistemas a los que afectan. Los administradores pueden programar las actualizaciones que se producirán durante las horas no pico.

La administración de vulnerabilidades identifica, clasifica, corrige y mitiga vulnerabilidades en sistemas y aplicaciones. Las herramientas de gestión de vulnerabilidades, también conocidas como escáneres de vulnerabilidades, deben utilizarse para evaluar regularmente la red, los sistemas y las aplicaciones. Cualquier vulnerabilidad identificada debe ser investigada y las medidas de corrección o mitigación apropiadas tomadas. Nessus es un popular escáner de vulnerabilidad de código abierto en uso hoy en día. Al igual que los sistemas de gestión de parches y las aplicaciones antivirus, es necesario asegurarse de que los escáneres de vulnerabilidades tienen los últimos archivos de firma.

PROCESOS DE GESTIÓN DEL CAMBIO

Todas las redes evolucionan, crecen y cambian con el tiempo. Las empresas y sus procesos también evolucionan y cambian, lo cual es algo bueno. Pero gestione el cambio de manera estructurada para mantener un sentido común de propósito sobre los cambios. Siguiendo los pasos recomendados en un proceso formal, se puede evitar que el cambio se convierta en la cola que mueve al perro. Las siguientes son directrices para incluir como parte de cualquier directiva de control de cambios:

- Todos los cambios deben solicitarse formalmente. Se deben mantener los registros de cambios.
- Cada solicitud debe ser analizada para asegurarse de que apoya todos los objetivos y policías. Esto incluye el análisis de impacto de base y seguridad.
- Antes de la aprobación formal, deben revisarse todos los costos y efectos de los métodos de aplicación. Con los datos recopilados, los cambios deben aprobarse o denegarse.
- Después de que se aprueben, los pasos de cambio deben desarrollarse.
- Durante la implementación, se deben realizar pruebas incrementales y debe basarse en una estrategia de reserva predeterminada si es necesario. El

control de versiones debe utilizarse para realizar un seguimiento eficaz y controlar los cambios en una colección de entidades.

- La documentación completa debe ser producida y presentada con un informe formal a la administración.

Una de las principales ventajas de seguir este método es la capacidad de hacer uso de la documentación en la planificación futura. Las lecciones aprendidas se pueden aplicar e incluso el proceso en sí se puede mejorar a través del análisis.

ESTRATEGIAS DE RECUPERACIÓN

La identificación de los controles preventivos es el tercer paso de los pasos de continuidad del negocio, tal como se describe en NIST SP 800-34 R1. Si se identifican controles preventivos en el análisis de impacto empresarial (BIA), es posible que se mitiguen o eliminen desastres o eventos disruptivos. Estas medidas preventivas disuaden, detectan y/o reducen los impactos en el sistema. Los métodos preventivos son preferibles a las acciones que podrían ser necesarias para recuperar el sistema después de una interrupción si los controles preventivos son factibles y rentables.

En las secciones siguientes se describen los controles principales que las organizaciones pueden implementar como parte de la continuidad del negocio y la recuperación ante desastres, incluidos los sistemas redundantes, las instalaciones y la energía; tecnologías de tolerancia a fallos; seguro; copia de seguridad de datos; detección y extinción de incendios; alta disponibilidad; calidad del servicio; y la resiliencia del sistema.

Crear estrategias de recuperación

Las organizaciones deben crear estrategias de recuperación para todos los activos que son vitales para un funcionamiento exitoso. *Las* estrategias de recuperación de nivel superior identifican el orden en que se restauran los procesos y funciones. *Las* estrategias de recuperación a nivel de sistema definen cómo se va a restaurar un sistema en particular. Tenga en cuenta que las personas que mejor entienden el sistema deben definir estrategias de recuperación del sistema. Aunque el comité de planificación de continuidad del negocio (BCP) probablemente puede desarrollar las listas de recuperación priorizada y las estrategias de recuperación de alto nivel, los administradores del sistema y otro personal de TI deben participar en el desarrollo de estrategias de recuperación para activos de TI.

Las tareas de recuperación ante desastres incluyen procedimientos de recuperación, procedimientos de seguridad del personal y procedimientos de restauración. El plan general de recuperación empresarial debe requerir que se forme un comité para decidir el mejor curso de acción. Este comité del plan de recuperación recibe su dirección del comité del BCP y de la alta dirección.

Todas las decisiones relativas a la recuperación deben tomarse de antemano e incorporarse al plan de recuperación ante desastres (DRP). Cualquier plan y procedimiento que se desarrolle debe referirse a funciones o procesos, no a individuos específicos. Como parte de la planificación de recuperación ante desastres, el comité del plan de recuperación debe ponerse en contacto con los proveedores críticos con anticipación para asegurarse de que cualquier equipo o suministro puede ser reemplazado de manera oportuna.

Cuando se ha producido un desastre o un evento perturbador, el portavoz de la organización debe informar de las malas noticias en una conferencia de prensa de emergencia antes de que la prensa se entere de la noticia a través de otro canal. El DRP debe detallar cualquier directriz para manejar la prensa. El sitio de la conferencia de prensa de emergencia debe planificarse con anticipación.

Al reanudar las operaciones normales después de un evento disruptivo, la organización debe llevar a cabo una investigación exhaustiva si se desconoce la causa del evento. El personal debe tener en cuenta todos los costos relacionados con daños que se producen como resultado del evento. Además, deben adoptarse las medidas adecuadas para evitar nuevos daños materiales.

Lo común entre todos los planes de recuperación es que todos se vuelven obsoletos. Por este motivo, requieren pruebas y actualización.

Esta sección incluye una discusión sobre la categorización de las prioridades de recuperación de activos, la recuperación de procesos empresariales, la recuperación de instalaciones, la recuperación de suministros y tecnología, la recuperación del entorno de usuario, la recuperación de datos y el personal de capacitación.

Categorizar las prioridades de recuperación de activos

Como se describe en el Capítulo 1,los valores del objetivo de tiempo de recuperación (RTO), el tiempo de recuperación del trabajo (WRT) y los valores del objetivo del punto de recuperación (RPO) determinan qué soluciones de recuperación se seleccionan. Un RTO estipula la cantidad de tiempo que una organización necesitará para recuperarse de un desastre, y una RPO estipula la cantidad de datos que una organización puede perder cuando ocurre un desastre. Los valores RTO, WRT y RPO se derivan durante el proceso BIA.

En el desarrollo de la estrategia de recuperación, el comité del plan de recuperación toma el valor rto, WRT y RPO y determina las estrategias de recuperación que deben utilizarse para garantizar que la organización cumpla estos objetivos de BIA.

Los dispositivos, sistemas y aplicaciones críticos deben restaurarse antes que los dispositivos, sistemas o aplicaciones que no entran en esta categoría. Tenga en cuenta al clasificar sistemas que la mayoría de los sistemas críticos no se pueden restaurar mediante métodos manuales. El comité del plan de recuperación debe comprender las soluciones de copia de seguridad/restauración que están disponibles e implementar el sistema que

proporcionará recuperación dentro de los valores BIA y las restricciones de costos. La ventana de tiempo para la recuperación de las capacidades de procesamiento de datos se basa en la criticidad de las operaciones afectadas.

Recuperación de procesos empresariales

Como parte del PRD, el comité del plan de recuperación debe comprender las interrelaciones entre los procesos y los sistemas. Un proceso empresarial es una colección de tareas que produce un servicio o producto específico para un cliente o cliente determinado.

Por ejemplo, si la organización determina que un sistema de contabilidad es una aplicación crítica y el sistema de contabilidad se basa en una granja de servidores de base de datos, el DRP debe incluir el servidor de base de datos como un activo crítico. Aunque es posible que no sea necesario restaurar toda la granja de servidores de base de datos para restaurar el sistema de contabilidad crítico, es posible que al menos uno de los servidores de la granja de servidores sea necesario para un funcionamiento adecuado.

Los documentos de flujo de trabajo deben proporcionarse al comité del plan de recuperación para cada proceso empresarial. Como parte de la recuperación de los procesos empresariales, el comité del plan de recuperación también debe comprender las funciones y recursos necesarios del proceso, las herramientas de entrada y salida e interfaces con otros procesos empresariales.

Recuperación de suministro y tecnología

Aunque la recuperación de las instalaciones no suele ser una preocupación con desastres más pequeños o eventos disruptivos, casi todos los esfuerzos de recuperación suelen implicar la recuperación de suministros y tecnología. Las organizaciones deben asegurarse de que cualquier DRP incluya directrices y procedimientos para recuperar suministros y tecnología. Como parte de la recuperación de la oferta y la tecnología, el DRP debe incluir toda la información de contacto pertinente del proveedor en caso de que se compren nuevos suministros y activos tecnológicos.

El DRP debe incluir información de recuperación sobre los siguientes activos que deben restaurarse:

- Copia de seguridad de hardware
- Copia de seguridad de software
- recursos humanos
- Calefacción, ventilación y aire acondicionado (HVAC)
- Suministros
- documentación

Copia de seguridad de hardware

El hardware que debe incluirse como parte del DRP incluye equipos cliente, equipos servidor, enrutadores, conmutadores, firewalls y cualquier otro hardware que se ejecute en la red de la organización. El DRP debe incluir no sólo directrices y procedimientos para restaurar todos los datos en cada uno de estos dispositivos, sino también información sobre la restauración manual de estos sistemas si los sistemas están dañados o completamente destruidos. También deben identificarse los dispositivos heredados que ya no están disponibles en el mercado minorista.

Como parte de la preparación del DRP, el equipo del plan de recuperación debe determinar la cantidad de tiempo que tardarán los proveedores de hardware en proporcionar reemplazos para cualquier hardware dañado o destruido. Sin esta información documentada, cualquier plan de recuperación podría ser ineficaz debido a la falta de recursos. Es posible que las organizaciones necesiten explorar otras opciones, como la compra de sistemas redundantes y el almacenamiento en una ubicación alternativa, si los proveedores no pueden proporcionar hardware de reemplazo de manera oportuna. Cuando es posible reemplazar los dispositivos heredados, las organizaciones deben tomar medidas para reemplazarlos antes de que ocurra el desastre.

Copia de seguridad de software

Incluso si una organización tiene todos los dispositivos necesarios para restaurar su infraestructura, esos dispositivos son inútiles si las aplicaciones y el software que se ejecutan en los dispositivos no están disponibles. Las aplicaciones y el software incluyen cualquier sistema operativo, base de datos y utilidades que necesiten ejecutarse en el dispositivo.

Muchas organizaciones podrían pensar que este requisito se cumple si tienen una copia de seguridad en cinta, DVD, unidad flash, disco duro u otros medios de todo su software. Pero todo el software del que se realiza una copia de seguridad normalmente requiere que al menos un sistema operativo se ejecute en el dispositivo en el que se restaura. Estas copias de seguridad de datos a menudo también requieren que el software de administración de copia de seguridad se esté ejecutando en el dispositivo de copia de seguridad, ya sea un servidor o un dispositivo dedicado.

Todos los medios de instalación de software, service packs y otras actualizaciones necesarias deben almacenarse en una ubicación alternativa. Además, toda la información de licencia debe documentarse como parte del DRP. Por último, se deben realizar copias de seguridad frecuentes de las aplicaciones, ya sea a través del sistema de copia de seguridad interno de la aplicación o a través de alguna otra copia de seguridad de la organización. Una copia de seguridad solo es útil si se puede restaurar, por lo que el DRP debe documentar completamente todos los pasos implicados.

En muchos casos, las aplicaciones se compran a un proveedor de software y solo el proveedor de software entiende la codificación que se produce en las aplicaciones. Debido a que no hay garantías en el mercado actual, algunas organizaciones podrían decidir que necesitan asegurarse de que están protegidas contra la desaparición de un proveedor de software. Un depósito en garantía de software es un acuerdo mediante el cual se le da a un tercero el código fuente del software para asegurarse de que el cliente tiene acceso al código fuente si se producen ciertas condiciones para el proveedor de software, incluyendo bancarrota y desastre.

recursos humanos

Ninguna organización es capaz de operar sin personal. Un plan de emergencia de ocupantes aborda específicamente los procedimientos para minimizar la pérdida de vidas o lesiones cuando se produce una amenaza. El equipo de recursos humanos es responsable de contactar a todo el personal en caso de desastre. La información de contacto de todo el personal debe almacenarse in situ y fuera del sitio. Varios miembros del equipo de recursos humanos deben tener acceso a la información de contacto del personal. Recuerde que la seguridad del personal es siempre la principal preocupación. Todos los demás recursos deben protegerse sólo después de que el personal esté a salvo.

Una vez finalizado el evento inicial, el equipo de recursos humanos debe controlar la moral del personal y protegerse contra el estrés y el agotamiento de los empleados durante el período de recuperación. Si se ha producido un entrenamiento cruzado adecuado, se puede rotar a varios personal durante el proceso de recuperación. Cualquier DRP debe tener en cuenta la necesidad de proporcionar períodos de descanso adecuados para cualquier personal involucrado en el proceso de recuperación ante desastres. También debe incluir directrices sobre cómo reemplazar a cualquier personal que sea víctima del desastre.

La organización debe asegurarse de que los salarios y otros fondos al personal continúen durante y después del desastre. Dado que la financiación puede ser fundamental tanto para el personal como para las compras de recursos, los cheques autorizados y firmados deben almacenarse de forma segura fuera del sitio. La gestión de nivel inferior con los controles de acceso adecuados debe tener la capacidad de dispersar fondos mediante estas comprobaciones en caso de que la alta dirección no esté disponible.

También se debe crear un plan de sucesión ejecutiva para garantizar que la organización siga las medidas adecuadas para protegerse y continuar el funcionamiento.

Suministros

A menudo, los desastres afectan la capacidad de suministrar a una organización los recursos necesarios, incluyendo papel, cableado e incluso agua. La organización debe documentar los recursos que son vitales para sus operaciones diarias y los proveedores de los que se pueden obtener estos

recursos. Dado que los proveedores de suministros también pueden verse afectados por el desastre, se deben identificar proveedores alternativos.

documentación

Para que la recuperación ante desastres sea un éxito, el personal involucrado debe ser capaz de completar los procedimientos de recuperación adecuados. Aunque la documentación de todos estos procedimientos puede ser tediosa, es necesario asegurarse de que se produce la recuperación. Además, se debe pedir a cada departamento dentro de la organización que decida qué documentación departamental se necesita para llevar a cabo operaciones diarias. Esta documentación debe almacenarse en una ubicación central en el lugar y también se debe conservar una copia fuera del sitio. Se debe encargar al personal específico que se asegure de que esta documentación se cree, almacene y actualice según corresponda.

Recuperación del entorno del usuario

Todos los aspectos de la recuperación del entorno del usuario final deben incluirse como parte del DRP para garantizar que los usuarios finales puedan volver al trabajo lo antes posible. Como parte de esta recuperación del entorno de usuario, debe producirse una notificación del usuario final. Se debe notificar a los usuarios dónde y cuándo informar después de que se produzca un desastre.

La recuperación real del entorno de usuario debe producirse por etapas, con las funciones más críticas que se restauran primero. Los requisitos del usuario deben documentarse para garantizar que se restablezcan todos los aspectos del entorno de usuario. Por ejemplo, los usuarios de un departamento crítico podrían necesitar su propio equipo cliente. Es posible que estos mismos usuarios también necesiten tener acceso a una aplicación que se encuentra en un servidor. Si el servidor no se restaura, los usuarios no podrán realizar sus tareas laborales incluso si sus equipos cliente están disponibles.

Por último, se deben documentar los pasos manuales que se pueden utilizar para cualquier función. Debido a que hoy en día dependemos tanto de la tecnología, a menudo pasamos por alto los métodos manuales para realizar nuestras tareas laborales. Documentar estos métodos manuales puede garantizar que las operaciones todavía pueden producirse, incluso si se producen a una velocidad reducida.

Recuperación de datos

En la mayoría de las organizaciones, los datos son uno de los activos más críticos a la hora de recuperarse de un desastre. Los BCPs y drps deben incluir directrices y procedimientos para recuperar datos. Sin embargo, los equipos de operaciones deben determinar de qué datos se realiza una copia de seguridad, con qué frecuencia se realiza una copia de seguridad de los datos y el método de copia de seguridad utilizado. Así que mientras esta sección discute la copia de seguridad de datos, recuerde que los equipos BCP realmente no toman

ninguna decisión de copia de seguridad de datos. Los equipos de BCP se preocupan principalmente por garantizar que los datos de los que se realiza la copia de seguridad puedan restaurarse de manera oportuna.

En esta sección se describen los tipos y esquemas de copia de seguridad de datos que se usan, así como los métodos de copia de seguridad electrónica que las organizaciones pueden implementar.

Tipos y esquemas de copia de seguridad de datos

Para diseñar una solución de recuperación de datos adecuada, los profesionales de la seguridad deben comprender los diferentes tipos de copias de seguridad de datos que pueden producirse y cómo se usan estas copias de seguridad juntas para restaurar los entornos en tiempo real.

Para el examen CISSP, los profesionales de la seguridad deben comprender los siguientes tipos y esquemas de copia de seguridad de datos:

- Copia de seguridad completa
- Respaldo diferencial
- Copia de seguridad incremental
- Copia de seguridad
- Copia de seguridad diaria
- Copia de seguridad del registro de transacciones
- Primero en, primer esquema de rotación de salida
- Plan de rotación abuelo/padre/hijo

Las tres copias de seguridad de datos principales son copias de seguridad completas, copias de seguridad diferenciales y copias de seguridad incrementales. Para comprender estos tres tipos de copia de seguridad de datos, debe comprender el concepto de bits de archivo. Cuando se crea o actualiza un archivo, el bit de archivo del archivo está habilitado. Si se borra el bit de archivo, el archivo no se archivará durante la siguiente copia de seguridad. Si el bit de archivo está habilitado, el archivo se archivará durante la siguiente copia de seguridad.

Con una copia de seguridad completa, se realiza una copia de seguridad de todos los datos. Durante el proceso de copia de seguridad completa, se borra el bit de archivado para cada archivo. Una copia de seguridad completa tarda más tiempo y más espacio en completarse. Sin embargo, si una organización solo usa copias de seguridad completas, solo es necesario restaurar la copia de seguridad completa más reciente. Cualquier copia de seguridad que utilice una

copia de seguridad diferencial o incremental comenzará primero con una copia de seguridad completa como línea base. Una copia de seguridad completa es la más adecuada para el archivado fuera del sitio.

En una copia de seguridad diferencial, se realizará una copia de seguridad de todos los archivos que se han cambiado desde la última copia de seguridad completa. Durante el proceso de copia de seguridad diferencial, el bit de archivo para cada archivo no se borra. Una copia de seguridad diferencial puede variar desde tomar un corto tiempo y una pequeña cantidad de espacio hasta crecer tanto en el tiempo de copia de seguridad como en la cantidad de espacio que necesita con el tiempo. Cada copia de seguridad diferencial realizará una copia de seguridad de todos los archivos de la copia de seguridad diferencial anterior si no se ha producido una copia de seguridad completa desde ese momento. En una organización que usa un esquema completo/diferencial, se debe restaurar la copia de seguridad completa y solo se debe restaurar la copia de seguridad diferencial más reciente, lo que significa que solo se necesitan dos copias de seguridad.

Una copia de seguridad incremental hace una copia de seguridad de todos los archivos que se han cambiado desde la última copia de seguridad completa o incremental. Durante el proceso de copia de seguridad incremental, se borra el bit de archivado para cada archivo. Una copia de seguridad incremental normalmente tarda la menor cantidad de tiempo y espacio en completarse. En una organización que usa un esquema completo/incremental, se debe restaurar la copia de seguridad completa y cada copia de seguridad incremental posterior. Las copias de seguridad incrementales deben restaurarse en orden. Si su organización completa una copia de seguridad completa los domingos y una copia de seguridad incremental diaria de lunes a sábado, podrían ser necesarias hasta siete copias de seguridad para restaurar los datos. La Figura 7-10 compara los diferentes tipos de copias de seguridad.

Backup Type	Data Backed Up	Backup Time	Restore Time	Storage Space
Full Backup	All Data	Slowest	Fast	High
Incremental Backup	Only New/Modified Files/Folders	Fast	Moderate	Lowest
Differential Backup	All Data Since Last Full	Moderate	Fast	Moderate

Figura 7-10 Comparación de tipos de copia de seguridad

Las copias de seguridad y las copias de seguridad diarias son dos tipos de copia de seguridad especiales que no se consideran parte de ningún esquema de copia de seguridad programado regularmente porque no requieren ningún otro tipo de copia de seguridad para la restauración. Las copias de seguridad de copia son similares a las copias de seguridad normales, pero no restablecen el bit de archivo del archivo. Las copias de seguridad diarias usan la marca de tiempo de un archivo para determinar si necesita archivar. Las copias de seguridad diarias son populares en entornos de misión crítica donde se

requieren varias copias de seguridad diarias porque los archivos se actualizan constantemente.

Las copias de seguridad del registro de transacciones solo se utilizan en entornos donde es importante capturar todas las transacciones que se han producido desde la última copia de seguridad. Las copias de seguridad del registro de transacciones ayudan a las organizaciones a recuperarse a un momento determinado y se usan con mayor frecuencia en entornos de base de datos.

Aunque las unidades de cinta magnética todavía se utilizan para realizar una copia de seguridad de los datos, muchas organizaciones hoy en día copian de seguridad de sus datos en discos ópticos, incluidos CD-ROM, DVDs y discos Blu-ray; unidades magnéticas de alta capacidad y alta velocidad; medios basados en flash; u otros medios. No importa el medio utilizado, es importante retener copias de seguridad tanto in situ como fuera del sitio. Almacene copias de seguridad in situ en una caja fuerte o bóveda impermeable, resistente al calor y resistente al fuego.

Copia de seguridad electrónica

Las soluciones de copia de seguridad electrónicas realizan copias de seguridad de datos de forma más rápida y precisa que las copias de seguridad de datos normales y se implementan mejor cuando la información cambia con frecuencia.

Para el examen CISSP, debe estar familiarizado con los siguientes términos y soluciones de copia de seguridad electrónica:

- **Bóveda electrónica:** Copia archivos a medida que se producen modificaciones. Este método se produce en tiempo real.
- **Registro en diario remoto:** Copia el diario o el cierre de sesión de transacciones en una programación regular. Este método se produce en lotes.
- **Bóveda de cinta:** Crea copias de seguridad a través de una línea de comunicación directa en un sistema de copia de seguridad en una instalación fuera del sitio.
- **Gestión jerárquica del almacenamiento de información (HSM):** Almacena los datos a los que se accede con frecuencia en medios más rápidos y datos a los que se accede con menos frecuencia en medios más lentos.
- **Máquina de discos óptica:** Almacena datos en discos ópticos y utiliza la robótica para cargar y descargar los discos ópticos según sea necesario. Este método es ideal cuando se requiere disponibilidad las 24/7.

- **Replicación:** Copia datos de una ubicación de almacenamiento a otra. La replicación sincrónica usa actualizaciones de datos constantes para asegurarse de que las ubicaciones están cerca de la misma, mientras que la replicación asincrónica retrasa las actualizaciones en una programación predefinida.

Muchas empresas utilizan soluciones de replicación o backup en la nube. Cualquier organización que tenga en cuenta una solución en la nube debe investigar todas las implicaciones de seguridad de este tipo de implementación.

Personal de capacitación

Incluso si una organización toma las medidas para desarrollar los BCPs y DRPs más completos, estos planes son inútiles si el personal de la organización no tiene las habilidades para recuperar completamente los activos de la organización cuando ocurre un desastre. Se debe dar al personal el tiempo y los recursos monetarios adecuados para garantizar que se produzca una formación adecuada. Esto incluye permitir que el personal pruebe cualquier DRP.

La formación debe obtenerse tanto de fuentes internas como externas. Cuando cambian las tareas laborales o se contrata nuevo personal, deben establecerse políticas para garantizar que se produzca la transferencia adecuada de conocimientos.

Estrategias de almacenamiento de copia de seguridad

Como parte de cualquier plan de copia de seguridad, una organización también debe tener en cuenta la estrategia de almacenamiento de copia de seguridad o el esquema de rotación que usará. Las consideraciones de costos y las consideraciones de almacenamiento a menudo dictan que los medios de copia de seguridad se reutilizan después de un período de tiempo. Si esta reutilización no está planeada de antemano, los medios pueden volverse poco fiables debido al uso excesivo. Dos de los esquemas de rotación de respaldo más populares son los primeros, primero fuera y abuelo / padre / hijo.

En el primer esquema de salida (FIFO), la copia de seguridad más reciente se guarda en el medio más antiguo. Aunque este es el esquema de rotación más simple, no protege contra errores de datos. Si existe un error en los datos, es posible que la organización no tenga una versión de los datos que no contenga el error.

En el esquema abuelo/padre/hijo (GFS), se definen tres conjuntos de copias de seguridad. La mayoría de las veces estas tres definiciones son diarias, semanales y mensuales. Las copias de seguridad diarias son los hijos, los respaldos semanales son los padres, y las copias de seguridad mensuales son los abuelos. Cada semana, un hijo avanza al set de padre. Cada mes, un padre avanza al conjunto del abuelo.

La Figura 7-11 muestra una rotación típica de GFS de 5 días usando 21 cintas. Las cintas diarias suelen ser copias de seguridad diferenciales o incrementales. Las cintas semanales y mensuales deben ser una copia de seguridad completa.

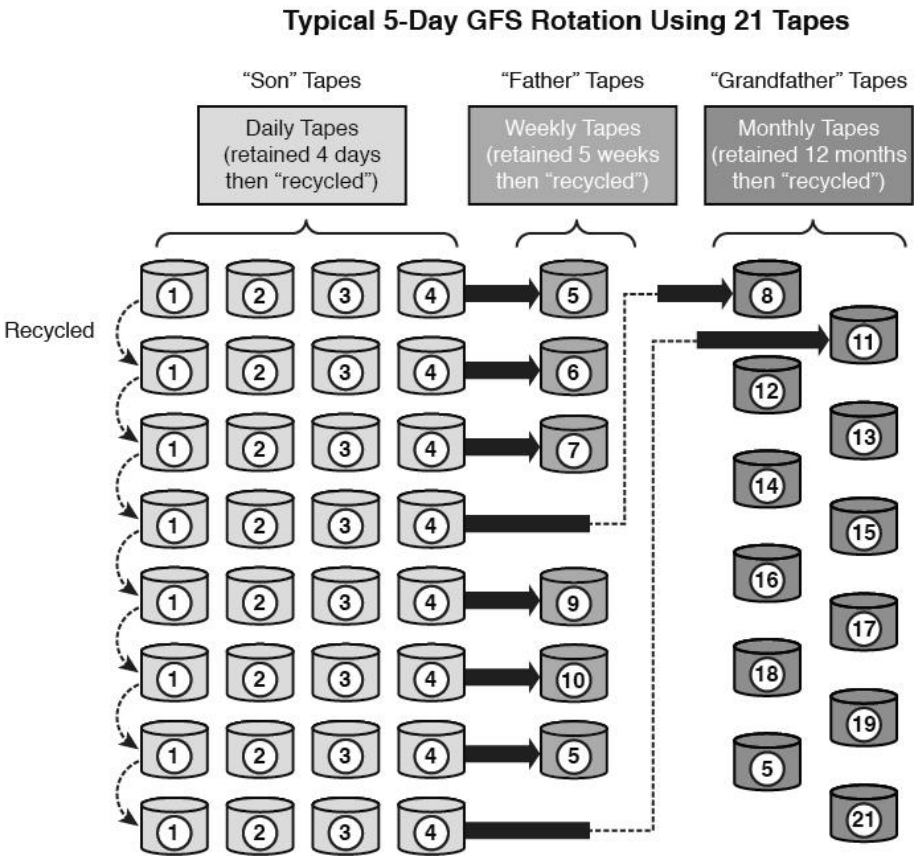

Figura 7-11 Abuelo/Padre/Hijo Esquema de Rotación de Respaldo

Recuperación y estrategias de múltiples sitios

Cuando se trata de un evento que destruye parcial o totalmente la instalación principal, la organización necesitará una ubicación alternativa desde la que operar hasta que se restablezca la instalación principal. El DRP debe definir la ubicación alternativa y sus procedimientos de recuperación, a menudo denominados estrategia de sitio de recuperación.

El DRP debe incluir no solo cómo llevar la ubicación alternativa a la operación completa, sino también cómo la organización volverá de la ubicación alternativa a la instalación principal después de restaurarla. Además, por motivos de seguridad, el DRP debe incluir detalles sobre los controles de seguridad que se usaron en la instalación principal y directrices sobre cómo implementar estos mismos controles en la ubicación alternativa.

El factor más importante para localizar una ubicación alternativa durante el desarrollo de la DRP es asegurarse de que la ubicación alternativa no se vea afectada por el mismo desastre. Esto puede significar que la organización debe seleccionar una ubicación alternativa que se encuentre en otra ciudad o región geográfica. Los principales factores que afectan a la selección de una ubicación alternativa incluyen los siguientes:

- Ubicación geográfica

- Necesidades organizativas
- Costo de la ubicación
- Esfuerzo de restauración de la ubicación

Probar una ubicación alternativa es una parte vital de cualquier DRP. Algunas ubicaciones son más fáciles de probar que otras. El PRD debe incluir instrucciones sobre cuándo y cómo probar periódicamente instalaciones alternativas para garantizar que la instalación de contingencia sea compatible con la instalación primaria.

Las ubicaciones alternativas que los profesionales de seguridad deben entender para el examen CISSP incluyen las siguientes:

- Sitio caliente
- Sitio frío
- Sitio cálido
- Sitio terciario
- Acuerdos recíprocos
- Sitios redundantes

Sitio caliente

Un sitio caliente es una instalación arrendada que contiene todos los recursos necesarios para el funcionamiento completo. Este entorno incluye computadoras, pisos elevados, servicios públicos completos, cableado eléctrico y de comunicaciones, equipos de red y UPS. El único recurso que se debe restaurar en un sitio caliente son los datos de la organización, a menudo solo parcialmente. Sólo debe tomar unas horas para llevar un sitio caliente a pleno funcionamiento.

Aunque un sitio caliente proporciona la recuperación más rápida, es el más caro de mantener. Además, puede ser administrativamente difícil de administrar si la organización requiere hardware o software propietario. Un sitio caliente requiere los mismos controles de seguridad que la instalación principal y la redundancia completa, incluido el hardware, el software y el cableado de comunicación.

Sitio frío

Un sitio frío es una instalación arrendada que contiene sólo cableado eléctrico y de comunicaciones, aire acondicionado, plomería y pisos elevados. No se instalan equipos de comunicaciones, hardware de red o computadoras en un sitio frío hasta que sea necesario para poner el sitio en funcionamiento. Por esta razón, un sitio frío tarda mucho más en restaurarse que un sitio caliente o cálido.

Aunque un sitio frío proporciona una recuperación más lenta, es el menos costoso de mantener. También es el más difícil de probar.

Sitio cálido

Un sitio cálido es una instalación arrendada que contiene cableado eléctrico y de comunicaciones, servicios públicos completos y equipos de red. En la mayoría de los casos, los únicos dispositivos que no están incluidos en un sitio cálido son los ordenadores. Un sitio cálido tarda más en restaurarse que un sitio caliente, pero menos que un sitio frío.

Un sitio cálido está en algún lugar entre el tiempo de restauración y el costo de un sitio caliente y sitio frío. Es la ubicación arrendada alternativa más ampliamente implementada. Aunque probar un sitio cálido es más fácil que probar un sitio frío, un sitio cálido requiere mucho más esfuerzo para las pruebas que un sitio caliente.

Figure 7-12 is a chart that compares the components deployed in these three sites.

	Hot Site	Warm Site	Cold Site
Electrical Connection	Yes	Yes	Yes
Peripherals	Yes	Some	None
Networking	Yes	None	None
Servers and Other Hardware	Yes	None	None
Applications	Yes	None	None

Figure 7-12 Hot Site, Warm Site, and Cold Site Comparison

Tertiary Site

A tertiary site is a secondary backup site that provides an alternate in case the hot site, warm site, or cold site is unavailable. Many large companies implement tertiary sites to protect against catastrophes that affect large geographic areas.

For example, if an organization requires a data center that is located on the coast, the organization might have its primary location in New Orleans, Louisiana, and its hot site in Mobile, Alabama. This organization might consider locating a tertiary site in Omaha, Nebraska, because a hurricane can affect both the Louisiana and Alabama Gulf coast.

Reciprocal Agreements

A reciprocal agreement is an agreement between two organizations that have similar technological needs and infrastructures. In the agreement, both organizations agree to act as an alternate location for the other if either of the organization's primary facilities are rendered unusable. Unfortunately in most cases, these agreements cannot be legally enforced.

A disadvantage of this site is that it might not be capable of handling the required workload and operations of the other organization.

> **Note**
>
> A mutual-aid agreement is a prearranged agreement between two organizations in which each organization agrees to provide assistance to the other in the event of a disaster.

Redundant Sites

A redundant or mirrored site is a site that is identically configured as the primary site. A redundant or mirrored site is not a leased site but is usually owned by the same organization as the primary site. The organization is responsible for maintaining the redundant site. Multiple processing sites can also be configured to serve as operationally redundant sites.

Although redundant sites are expensive to maintain, many organizations today see them as a necessary expense to ensure that uninterrupted service can be provided.

Redundant Systems, Facilities, and Power

In anticipation of disasters and disruptive events, organizations should implement redundancy for critical systems, facilities, and power and assess any systems that have been identified as critical to determine whether implementing redundant systems is cost effective. Implementing redundant systems at an alternate location often ensures that services are uninterrupted. Redundant systems include redundant servers, redundant routers, redundant internal hardware, and even redundant backbones. Redundancy occurs when an organization has a secondary component, system, or device that takes over when the primary unit fails.

Redundant facilities ensure that the organization maintains a facility at whatever level it chooses to ensure that the organizational services can continue when a disruptive event occurs. Redundant facilities are discussed in more depth elsewhere in this chapter.

Power redundancy is implemented using uninterruptible power supplies (UPSs) and power generators.

Redundancy on individual components can also be provided. The spare components are either cold spares, warm spares, or hot spares. A cold spare is not powered up but can be inserted into the system if needed. A warm spare is in the system but does not have power unless needed. A hot spare is in the system and powered on, ready to become operational at a moment's notice.

Fault-Tolerance Technologies

La tolerancia a errores permite a un sistema continuar el funcionamiento en caso de error de uno o varios componentes. La tolerancia a errores dentro de un sistema puede incluir tarjetas adaptadoras tolerantes a errores y unidades de almacenamiento tolerantes a errores. Uno de los sistemas de tolerancia a errores más conocidos es RAID, que se discute anteriormente en este capítulo.

Mediante la implementación de tecnologías tolerantes a errores, una organización puede asegurarse de que se produce un funcionamiento normal si se produce un error en un único componente tolerante a errores.

seguro

Aunque la redundancia y la tolerancia a fallos pueden actuar como medidas preventivas contra las fallas, el seguro no es realmente una medida preventiva. Si una organización compra un seguro para proporcionar protección en caso de un evento disruptivo, el seguro no tiene poder para protegerse contra el evento en sí. El propósito del seguro es asegurar que la organización tendrá acceso a recursos financieros adicionales para ayudar en la recuperación.

Tenga en cuenta que los esfuerzos de recuperación de un evento disruptivo a menudo pueden incurrir en grandes costos financieros. Incluso algunas de las mejores estimaciones todavía podrían quedarse cortas cuando la recuperación real debe tener lugar. Al comprar un seguro, la organización puede asegurarse de que se cubran las transacciones financieras clave, incluidos los gastos de nómina, las cuentas por pagar y los costes de recuperación.

La valoración de costes reales del seguro (ACV) compensa la propiedad en función del valor del artículo en la fecha de pérdida más el 10 por ciento. Sin embargo, tenga en cuenta que el seguro de cualquier material impreso solo cubre documentos, manuscritos o registros inscritos, impresos o escritos. No cubre dinero y valores. Un tipo especial de seguro llamado seguro de *interrupción del negocio* proporciona protección monetaria para los gastos y pérdida de ganancias.

Las organizaciones deben revisar anualmente las pólizas de seguro y actualizarlas según sea necesario.

Copia de seguridad de datos

La copia de seguridad de datos proporciona prevención contra la pérdida de datos, pero no la prevención contra el evento disruptivo. Todas las organizaciones deben asegurarse de que todos los sistemas que almacenan archivos importantes se realizan de forma oportuna. También se debe animar a los usuarios a realizar una copia de seguridad de los archivos personales que puedan necesitar. Además, deben realizarse pruebas periódicas del proceso de restauración para garantizar la restauración de los archivos.

La recuperación de datos, incluidos los tipos y esquemas de copia de seguridad y el respaldo electrónico, se cubrió en detalle anteriormente en este capítulo.

Detección y supresión de incendios

Las organizaciones deben implementar sistemas de detección y supresión de incendios como parte de cualquier BCP. La detección y supresión de incendios varían en función del método de detección/supresión utilizado y se discuten con mayor detalle en la sección"Seguridad ambiental"del capítulo 3.

alta disponibilidad

La alta disponibilidad en la recuperación de datos es un concepto que garantiza que los datos estén siempre disponibles mediante redundancia y tolerancia a errores. La mayoría de las organizaciones implementan soluciones de alta disponibilidad como parte de cualquier DRP.

Los términos y técnicas de alta disponibilidad que debe comprender incluyen los siguientes:

- **Matriz redundante de discos independientes (RAID):** Una tecnología de disco duro en la que los datos se escriben en varios discos de tal manera que un disco puede fallar y los datos se pueden hacer disponibles rápidamente desde los discos restantes de la matriz sin restaurarlos desde una cinta de copia de seguridad u otros medios de copia de seguridad.

- **Red de área de almacenamiento (SAN):** Dispositivos de almacenamiento de alta capacidad conectados por una red privada de alta velocidad mediante conmutadores específicos del almacenamiento.

- **Conmutación por error:** La capacidad de un sistema para cambiar a un sistema de copia de seguridad si se produce un error en el sistema primario.

- **Failsoft:** La capacidad de un sistema para terminar procesos no críticos cuando se produce un error.

- **Agrupación en clústeres:** Hace referencia a un producto de software que proporciona servicios de equilibrio de carga. Con la agrupación en clústeres, una instancia de un servidor de aplicaciones actúa como controlador maestro y distribuye solicitudes a varias instancias mediante algoritmos round robin, round robin ponderado o de conexiones de menor.

- **Equilibrio de carga:** Hace referencia a un producto de hardware que proporciona servicios de equilibrio de carga. Los controladores de entrega de aplicaciones (ADC) admiten los mismos algoritmos, pero también utilizan procesos complejos de contracción de números, como cpu por servidor y utilización de memoria, tiempos de respuesta más rápidos, etc., para ajustar el equilibrio de la carga. Las soluciones de equilibrio de carga también se conocen como granjas de servidores o grupos.

Calidad del servicio

La calidad del servicio (QoS) es una tecnología que administra los recursos de red para garantizar un nivel de servicio predefinido. Asigna las prioridades de tráfico a los diferentes tipos de tráfico o protocolo en una red. QoS se implementa cuando se produce un cuello de botella y decide qué tráfico es más importante que el resto. Exactamente qué tráfico es más importante que qué otro tráfico se basa en las reglas que el administrador suministra. La importancia se puede basar en la dirección IP, la dirección MAC e incluso el nombre del servicio. Sin embargo, QoS solo funciona cuando se produce un cuello de botella en la ubicación adecuada y la configuración son las declaraciones de ancho de banda. Por ejemplo, si las configuraciones de QoS se fijan más allá del ancho de banda del ISP, el tráfico no será priorizado si un router piensa que hay suficiente ancho de banda disponible. Pero, ¿qué pasa si se están cumpliendo los máximos del ISP y el ISP decide qué es o no importante? La clave de cualquier implementación de QoS es ajustar la configuración y observar la red a lo largo del tiempo.

Resiliencia del sistema

La resiliencia del sistema es la capacidad de un sistema, dispositivo o centro de datos para recuperarse rápidamente y continuar operando después de un fallo del equipo, un corte de energía u otra interrupción. Implica el uso de componentes o instalaciones redundantes. Cuando un componente falla o se interrumpe, el componente redundante toma el control sin problemas y continúa proporcionando servicios a los usuarios.

RECUPERACIÓN ANTE DESASTRES

La recuperación ante desastres implica restaurar los servicios y sistemas desde un estado de contingencia, o el estado temporal de que las operaciones pueden estar en donde se están ejecutando, pero no en la instalación primaria o en los recursos óptimos. El PRD se examina en detalle en el capítulo 1. En este capítulo, hablamos más sobre el proceso de recuperación ante desastres, en términos de respuesta, personal, comunicaciones, evaluación, restauración y capacitación y sensibilización.

respuesta

Una vez ocurrido el suceso, se debe contactar con el personal correspondiente para iniciar las comunicaciones que alerten al equipo de recuperación correspondiente y al personal afectado del suceso. Todos los equipos enumerados en la sección de personal entonces necesitan realizar sus funciones. Se debe desarrollar una jerarquía de procesos para que cada equipo realice sus deberes como parte del proceso de recuperación ante desastres en el orden correcto.

personal

Aunque las prioridades número uno y número dos cuando se produce un desastre son la seguridad del personal y la mitigación de daños y salud, respectivamente, recuperarse de un desastre rápidamente se convierte en la

prioridad de una organización después de que se manejan estos dos. Sin embargo, ninguna organización puede recuperarse de un desastre si el personal no está debidamente capacitado y preparado. Para garantizar que el personal pueda desempeñar sus funciones durante la recuperación ante desastres, debe conocer y comprender sus tareas laborales.

Durante cualquier recuperación ante desastres, la gestión financiera es importante. La gestión financiera generalmente incluye al director financiero y a cualquier otro personal contable clave. Este grupo debe realizar un seguimiento de los costes de recuperación y evaluar las proyecciones de flujo de caja. Notifican formalmente a cualquier aseguradora de reclamaciones que se harán. Por último, este grupo es responsable de establecer directrices de continuidad de nóminas, procedimientos de contratación y procedimientos de seguimiento de costos de emergencia.

Las organizaciones deben decidir qué equipos son necesarios durante una recuperación ante desastres y asegurarse de que el personal adecuado se coloca en cada uno de estos equipos. El administrador de recuperación ante desastres dirige las acciones de recuperación a corto plazo inmediatamente después de un desastre.

Es posible que las organizaciones deba implementar los siguientes equipos para proporcionar el soporte adecuado para el DRP:

- Equipo de evaluación de daños
- Equipo legal
- Equipo de relaciones con los medios
- Equipo de recuperación
- Equipo de reubicación
- Equipo de restauración
- Equipo de salvamento
- Equipo de seguridad

Equipo de evaluación de daños

El equipo de evaluación de daños es responsable de determinar la causa del desastre y la cantidad de daño que se ha producido a los activos de la organización. Identifica todos los activos afectados y la funcionalidad de los activos críticos después del desastre. El equipo de evaluación de daños determina qué activos tendrán que ser restaurados y reemplazados y se pone en contacto con los equipos apropiados que necesitan ser activados.

Equipo legal

El equipo legal se ocupa de todos los asuntos legales inmediatamente después del desastre y durante la recuperación del desastre. El equipo legal supervisa cualquier evento de relaciones públicas que se celebre para abordar el desastre, aunque el equipo de relaciones con los medios de comunicación realmente entregará el mensaje. El equipo legal debe ser consultado para asegurar que todas las operaciones de recuperación se adhieran a las leyes y regulaciones federales y estatales.

Equipo de Relaciones con los Medios

El equipo de relaciones con los medios de comunicación informa al público y a los medios de comunicación cada vez que las emergencias se extienden más allá de las instalaciones de la organización de acuerdo con las directrices dadas en el PRD. El sitio de la conferencia de prensa de emergencia debe ser planeado con anticipación. Al emitir declaraciones públicas, el equipo de relaciones con los medios de comunicación debe ser honesto y preciso sobre lo que se sabe sobre el evento y sus efectos. La respuesta de la organización a los medios de comunicación durante y después del evento debe unificarse.

Un portavoz creíble e informado debe dar la respuesta de la organización. Cuando se trata de los medios de comunicación después de un desastre, el portavoz debe informar de malas noticias antes de que los medios lo descubran a través de otro canal. Cualquiera que haga anuncios de desastre al público debe entender que la audiencia para tales anuncios incluye a los medios de comunicación, sindicatos, partes interesadas, vecinos, empleados, contratistas e incluso competidores.

Equipo de recuperación

La tarea principal del equipo de recuperación es recuperar las funciones empresariales críticas en la instalación alternativa. Esto implica principalmente asegurar que los activos físicos están en su lugar, incluyendo computadoras y otros dispositivos, cableado, etc. El equipo de recuperación generalmente supervisa los equipos de reubicación y restauración.

Equipo de reubicación

El equipo de reubicación supervisa la transferencia real de activos entre ubicaciones. Esto incluye mover activos del sitio primario al sitio alternativo y, a continuación, devolver esos activos cuando el sitio principal está listo para funcionar.

Equipo de restauración

El equipo de restauración realmente se asegura de que los activos y datos se restablezcan en las operaciones. El equipo de restauración necesita acceso a los medios de copia de seguridad.

Equipo de salvamento

El equipo de salvamento recupera todos los activos en la ubicación del desastre y se asegura de que el sitio primario vuelva a la normalidad. El equipo de

rescate gestiona la limpieza de los equipos, supervisa la reconstrucción de la instalación original e identifica a cualquier experto para emplear en el proceso de recuperación. En la mayoría de los casos, el equipo de rescate declara cuándo se pueden reanudar las operaciones en el lugar del desastre.

Equipo de seguridad

El equipo de seguridad es responsable de administrar la seguridad tanto en el sitio de desastres como en cualquier ubicación alternativa que la organización use durante la recuperación. Debido a que el área geográfica que el equipo de seguridad debe administrar después del desastre es a menudo mucho más grande, el equipo de seguridad podría necesitar contratar contratistas externos para ayudar en este proceso. El uso de estos contratistas externos para proteger el acceso físico a los sitios y el uso de recursos internos para proporcionar seguridad dentro de las instalaciones siempre es mejor porque el estado reducido podría dificultar la emisión de la credencial de acceso adecuada a los contratistas.

Comunicaciones

La comunicación durante la recuperación ante desastres es importante para garantizar que la organización se recupere en tiempo y forma. También es importante asegurarse de que no se omiten los pasos y que los pasos ocurran en el orden correcto. La comunicación con el personal depende de quién esté siendo contactado sobre el desastre. El personal afectado por un desastre debe recibir comunicaciones que enumere los sistemas afectados, el tiempo de interrupción proyectado y cualquier contingencia que deban seguir mientras tanto. Los diferentes equipos de recuperación ante desastres deben recibir comunicaciones relacionadas con sus funciones durante la recuperación del desastre.

Durante la recuperación, los profesionales de la seguridad deben trabajar en estrecha colaboración con los diferentes equipos para garantizar que todos los activos permanezcan seguros. Todos los equipos involucrados en el proceso también deben comunicarse a menudo entre sí para actualizarse mutuamente sobre el progreso.

evaluación

Cuando se produce un evento, el personal debe evaluar la gravedad y el impacto del evento. Al hacerlo, se garantiza que se implemente la respuesta adecuada. La mayoría de las organizaciones establecen categorías de eventos, incluidos incidentes, incidentes e incidentes graves. Cada organización debe tener un proceso de evaluación de recuperación ante desastres para garantizar que el personal evalúe adecuadamente cada evento.

restauración

El proceso de restauración implica restaurar los sistemas e instalaciones primarios al funcionamiento normal. El personal involucrado en este proceso depende de los activos que se vieron afectados por el evento. Cualquier equipo

involucrado en la recuperación de activos debe coordinar cuidadosamente sus esfuerzos de recuperación. Sin una coordinación cuidadosa, la recuperación podría verse afectada negativamente. Por ejemplo, si la recuperación completa de una aplicación web requiere que los servidores de base de datos estén operativos, el administrador de la base de datos debe trabajar estrechamente con el administrador de la aplicación web para asegurarse de que ambos se devuelven a la función normal.

Formación y sensibilización

El personal de todos los niveles debe recibir la capacitación adecuada sobre el proceso de recuperación ante desastres. Los usuarios regulares sólo necesitan recibir capacitación de concienciación para que entiendan la complejidad del proceso. El liderazgo necesita capacitación sobre cómo dirigir la organización durante una crisis. Los equipos técnicos necesitan capacitación sobre los procedimientos de recuperación y logística. Los profesionales de la seguridad necesitan capacitación sobre cómo proteger los activos durante la recuperación.

La mayoría de las organizaciones incluyen la continuidad del negocio y la capacitación de concienciación sobre la recuperación ante desastres como parte de la capacitación inicial que se da al personal cuando son contratados. Las organizaciones también deben actualizar periódicamente el personal para asegurarse de que no se olviden de la recuperación ante desastres.

> **nota**
>
> La continuidad del negocio y la recuperación ante desastres se tratan con más detalle en el capítulo 1.

PRUEBAS DE PLANES DE RECUPERACIÓN ANTE DESASTRES

Después de que el BCP esté completamente documentado, una organización debe tomar medidas para asegurarse de que el plan se mantiene y se mantiene actualizado. Como mínimo, una organización debe evaluar y modificar el BCP y el DRP anualmente. Esta evaluación generalmente implica algún tipo de prueba para asegurar que los planes sean precisos y exhaustivos. Las pruebas con frecuencia son importantes porque cualquier plan no es viable a menos que se haya realizado una prueba. A través de pruebas, se detectan imprecisiones, deficiencias y omisiones.

Las pruebas del BCP y el DRP preparan y capacitan al personal para que desempeñe sus funciones. También garantiza que el sitio de copia de seguridad alternativo pueda funcionar según sea necesario. Cuando se realizan pruebas, la prueba probablemente es defectuosa si no se encuentran problemas con el plan.

Los tipos de pruebas que se utilizan comúnmente para evaluar el BCP y el DRP incluyen los siguientes:

- Prueba de lectura
- Prueba de lista de verificación
- Ejercicio de mesa
- Prueba estructurada
- Prueba de simulación
- Prueba paralela
- Prueba de interrupción completa
- Taladro funcional
- Simulacro de evacuación

Prueba de lectura

Una prueba de lectura implica a los equipos que forman parte de cualquier plan de recuperación. Estos equipos leen el plan que se ha desarrollado e intentan identificar cualquier inexactitud u omisión en el plan.

Prueba de lista de verificación

La prueba de lista de comprobación se produce cuando los administradores de cada departamento o área funcional revisan el BCP. Estos gerentes hacen nota de cualquier modificación del plan. A continuación, el comité BCP utiliza todas las notas de gestión para realizar cambios en el BCP.

Ejercicio de mesa superior

Un ejercicio de mesa es la forma más rentable y eficiente de identificar áreas de superposición en el plan antes de realizar pruebas de nivel superior. Un ejercicio de mesa es una sesión informal de lluvia de ideas que fomenta la participación de líderes empresariales y otros empleados clave. En un ejercicio de mesa, los participantes están de acuerdo con un escenario de desastre en particular en el que se centrarán.

Prueba estructurada de walk-through

La prueba estructurada implica que representantes de cada departamento o área funcional revisen a fondo la exactitud del BCP. Este tipo de prueba es la prueba más importante que se debe realizar antes de un desastre en vivo.

Prueba de simulación

En una prueba de simulación, las operaciones y el personal de soporte ejecutan el DRP en un escenario de juego de roles. Esta prueba identifica los pasos y amenazas omitidos.

Prueba paralela

Una prueba paralela implica llevar el sitio de recuperación a un estado de preparación operativa pero mantener las operaciones en el sitio primario.

Prueba de interrupción completa

Una prueba de interrupción completa implica cerrar la instalación primaria y llevar la instalación alternativa a su máxima operación. Este es un switch-over duro en el que todo el procesamiento ocurre en la instalación primaria hasta que se lanza el "Switch". Este tipo de prueba requiere una coordinación completa entre todas las partes e incluye notificar a los usuarios antes de la prueba planificada. Una organización debe realizar este tipo de prueba solo cuando se hayan implementado todas las demás pruebas y se hayan realizado correctamente.

Taladro funcional

Un taladro funcional prueba una sola función o departamento para ver si el DRP de la función está completo. Este tipo de simulacro requiere la participación del personal que realiza la función.

Simulacro de evacuación

En un simulacro de evacuación, el personal sigue las directrices de evacuación o refugio en el lugar para un tipo de desastre en particular. En este tipo de simulacro, el personal debe comprender el área a la que debe informar cuando se produce la evacuación. Todo el personal debe ser contabilizado en ese momento.

PLANIFICACIÓN Y EJERCICIOS DE CONTINUIDAD DEL NEGOCIO

Una vez completada una prueba, todos los resultados de las pruebas deben documentarse y los planes deben modificarse para reflejar esos resultados. La lista de actividades exitosas y infructuosas de las pruebas será la más útil para la administración al mantener el BCP. Toda la información obsoleta de los planes debe eliminarse y se debe agregar cualquier nueva información. Además, podría ser necesario modificar la información actual basada en nuevas regulaciones, leyes o protocolos.

El control de versiones de los planes debe administrarse para garantizar que la organización siempre usa la versión más reciente. Además, el BCP debe almacenarse en varias ubicaciones para asegurarse de que está disponible si el desastre destruye una ubicación. El personal múltiple debe tener la versión más reciente de los planes para asegurarse de que los planes se pueden recuperar si el personal primario no está disponible cuando se necesita el plan.

SEGURIDAD FÍSICA

La seguridad física implica el uso de los controles de seguridad adecuados para proteger todos los activos del acceso físico. La seguridad perimetral implica la implementación de los controles de seguridad perimetrales adecuados, incluyendo puertas y vallas, detección de intrusiones perimetrales, iluminación, patrullaje y control de acceso, para evitar el acceso al perímetro de una instalación. La construcción y la seguridad interna implican la implementación de los controles de construcción y seguridad interna adecuados.

Controles de seguridad perimetral

Al considerar la seguridad perimetral de una instalación, tomar un enfoque holístico, a veces conocido como el enfoque *de círculo concéntrico,* a veces es útil (consulte la Figura 7-13). Este enfoque se basa en la creación de capas de barreras físicas a la información.

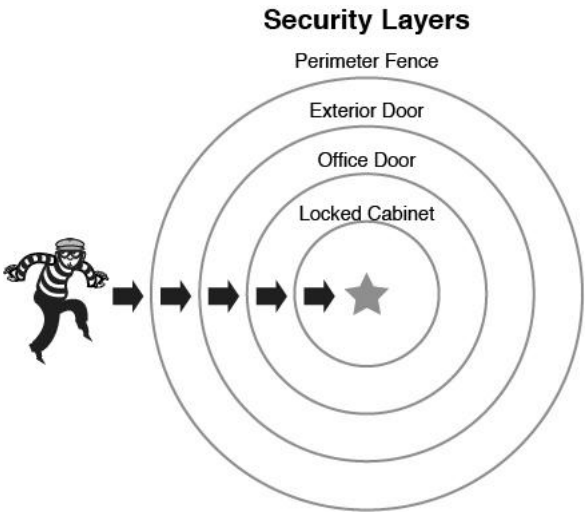

Figura 7-13 Enfoque de círculo concéntrico

En esta sección, analizaremos la implementación de este concepto en detalle.

Puertas y vallas

El anillo más exterior en el enfoque de círculo concéntrico se compone de las puertas y vallas que rodean la instalación. Dentro de ellos hay círculos interiores de barreras físicas, cada uno de los cuales tiene su propio conjunto de preocupaciones. En este apartado, se cubren las consideraciones de barreras (bolardos), vallas, puertas y muros.

Barreras (Bolardos)

Las barreras llamadas *bolardos* se han vuelto bastante comunes alrededor del perímetro de nuevas oficinas y edificios gubernamentales. Se trata de postes verticales cortos colocados en la entrada del edificio y aceras de revestimiento que ayudan a proporcionar protección contra vehículos que podrían chocar intencional o involuntariamente o entrar en el edificio o herir a los peatones.

Se pueden hacer de muchos tipos de materiales. Los que se muestran en la Figura 7-14 son de acero inoxidable.

Figura 7-14 Bolardos de acero inoxidable

Cercas

La esgrima es la primera línea de defensa en el paradigma del círculo concéntrico. Al seleccionar el tipo de cerca para instalar, considere la determinación de la persona que está tratando de desalentar. Utilice las siguientes directrices con respecto a la altura:

- Las vallas de 3 a 4 pies de altura disuaden sólo a los intrusos casuales.
- Las vallas de 6 a 7 pies de altura son demasiado altas para escalar fácilmente.
- Vallas de 8 pies y disuasión más alta intrusos más determinados, especialmente cuando se aumenta con alambre de afeitar.

Una geo-cerca es un área geográfica dentro de la cual los dispositivos se gestionan utilizando algún tipo de comunicación de radiofrecuencia. Por ejemplo, se podría configurar una geo-cerca en un radio alrededor de una tienda o ubicación de punto o dentro de un conjunto predefinido de límites, como alrededor de una zona escolar. Se utiliza para rastrear a los usuarios o dispositivos que entran o salen del área de geo-cerca. Las alertas se pueden configurar para enviar mensajes al usuario del dispositivo y al operador de geo-vallado de la ubicación del dispositivo.

portones

Las puertas pueden ser puntos débiles en una valla si no se manejan correctamente. Gates son calificados por el Laboratorio de Suscriptores (UL) de la siguiente manera. Cada paso adelante en la clase requiere niveles adicionales de protección:

- **Clase 1:** Uso residencial
- **Clase 2:** Uso comercial
- **Clase 3:** Uso industrial
- **Clase 4:** Área restringida

paredes

En algunos casos, se podrían pedir muros alrededor de una instalación. Cuando ese es el caso, y cuando la seguridad perimetral es crítica, los sistemas de detección de intrusiones perimetrales, que se describen a continuación, se pueden implementar para alertarle de cualquier rotura de los muros.

Detección de intrusiones perimetrales

Independientemente de si utiliza vallas o muros, o incluso si decide implementar ninguno de estos impedimentos, puede reducir significativamente su exposición mediante la implementación de uno de los siguientes tipos de sistemas de detección de intrusiones perimetrales. Todos los sistemas descritos a continuación se consideran métodos de detección de intrusiones físicas.

Sensores infrarrojos

Los sistemas infrarrojos pasivos (PIR) funcionan identificando cambios en las ondas de calor en un área. Debido a que la presencia de un intruso elevaría la temperatura de las partículas de aire circundantes, este sistema alerta o suena una alarma cuando esto ocurre.

Sistemas electromecánicos

Los sistemas electromecánicos funcionan mediante la detección de una rotura en un circuito eléctrico. Por ejemplo, el circuito puede cruzar una ventana o puerta y cuando se abre la ventana o la puerta, el circuito está roto, activando una alarma de algún tipo. Otro ejemplo podría ser una almohadilla de presión colocada debajo de la alfombra para detectar la presencia de individuos.

Sistemas fotoeléctricos

Los sistemas fotométricos o fotoeléctricos funcionan detectando cambios en la luz y, por lo tanto, se utilizan en áreas sin ventanas. Envían un haz de luz a través de la zona, y si la viga es interrumpida (por una persona, por ejemplo), se activa la alarma.

Sistemas de detección acústica

Los sistemas acústicos utilizan micrófonos estratégicamente colocados para detectar cualquier sonido realizado durante una entrada forzada. Estos sistemas sólo funcionan bien en áreas donde no hay mucho ruido circundante. Por lo general, son muy sensibles, lo que causaría muchas falsas alarmas en un área ruidosa, como una puerta al lado de una calle concurrida.

Detector de movimiento de onda

Estos dispositivos generan un patrón de onda en el área y detectan cualquier movimiento que moleste el patrón de onda. Cuando el patrón es perturbado, suena una alarma.

Detector de capacitancia

Estos dispositivos emiten un campo magnético y monitorean ese campo. Si el campo se interrumpe, lo que ocurrirá cuando una persona entre en el área, la alarma sonará.

Cctv

Un sistema de televisión de circuito cerrado (CCTV) utiliza conjuntos de cámaras que pueden ser monitoreadas en tiempo real o pueden registrar días de actividad que se pueden ver según sea necesario en un momento posterior. En instalaciones de muy alta seguridad, estos suelen ser monitoreados. Uno de los principales beneficios del uso de CCTV es que aumenta las capacidades visuales del guardia. Los guardias pueden monitorear áreas más grandes a la vez desde un lugar central. CCTV es una categoría de vigilancia física, no de vigilancia informática/de red.

Los tipos de cámara incluyen cámaras al aire libre, cámaras infrarrojas, cámaras de posición fija, cámaras de panorámica/inclinación, cámaras domo y cámaras de protocolo de Internet (IP). Al implementar cámaras, las organizaciones deben seleccionar la lente, resolución, fotogramas por segundo (FPS) y compresión adecuados. Además, debe entenderse el análisis de los requisitos de iluminación de las diferentes cámaras; un sistema cctv debe funcionar en la cantidad de luz que proporciona la ubicación. Además, una organización debe comprender el tipo diferente de pantallas de monitor, incluidas las pantallas de una sola imagen, la pantalla dividida y las pantallas de gran formato.

iluminación

Una de las mejores maneras de disuadir el crimen y las travesuras es arrojar luz sobre las áreas de preocupación. En esta sección, nos fijamos en algunos tipos de iluminación y algunos sistemas de iluminación que han demostrado ser eficaces. La iluminación se considera un control físico para la seguridad física.

Tipos de sistemas

El profesional de la seguridad debe estar familiarizado con varios tipos de sistemas de iluminación:

- **Iluminación continua:** Una serie de luces que proporcionan una cantidad uniforme de iluminación a través de un área
- **Iluminación en espera:** Un tipo de sistema que se ilumina sólo en ciertos momentos o en un horario
- **Iluminación móvil:** Iluminación que se puede reposicionar según sea necesario
- **Iluminación de emergencia:** Sistemas de iluminación con su propia fuente de alimentación para usar cuando se apague la energía

Tipos de iluminación

Una serie de opciones están disponibles al elegir la fuente de iluminación o el tipo de luz. Las siguientes son las opciones más comunes:

- **Fluorescente:** Una lámpara de descarga de gas-vapor de mercurio y vapor de muy baja presión que utiliza fluorescencia para producir luz visible.
- **Vapor de mercurio:** Una lámpara de descarga de gas que utiliza un arco eléctrico a través de mercurio vaporizado para producir luz.
- **Vapor de sodio:** Una lámpara de descarga de gas que utiliza sodio en estado excitado para producir luz.
- **Lámparas de cuarzo:** Una lámpara que consiste en una fuente de luz ultravioleta, como el vapor de mercurio, contenida en una bombilla de sílice fusionada que transmite luz ultravioleta con poca absorción.

Independientemente de la fuente de luz, será calificada por sus *pies de iluminación*. Al colocar las luces, debe tener en cuenta esta calificación. Por ejemplo, si un accesorio de luz controlado montado en un poste de 5 metros puede iluminar un área de 30 metros de diámetro, con fines de iluminación de seguridad, la distancia entre las luminarias debe ser de 30 pies. Además, debe haber una amplia iluminación perimetral exterior de entradas o zonas de aparcamiento para desalentar a los merodeos o intrusos ocasionales.

Fuerza de patrulla

Un excelente aumento a todos los demás sistemas de detección es la presencia de un guardia que patrulla las instalaciones. Esta opción ofrece la mayor flexibilidad para reaccionar a lo que ocurra. Una de las claves del éxito es la adecuada capacitación de los guardias para que estén preparados para cualquier eventualidad. Debe haber una respuesta preparada para cualquier posible ocurrencia. Uno de los principales beneficios de este enfoque es que los guardias pueden utilizar el juicio discriminatorio basado en la situación, lo que los sistemas automatizados no pueden hacer.

La fuerza de patrulla puede ser contratada internamente, entrenada y controlada o puede ser subcontratada a una compañía de seguridad

contractual. Una organización puede controlar la capacitación y el rendimiento de una fuerza de patrulla interna. Sin embargo, algunas organizaciones subcontratan la fuerza de patrulla para garantizar la imparcialidad.

control de acceso

Al conceder acceso físico a la instalación, deben seguirse una serie de directrices con respecto al mantenimiento de registros. Todo intento exitoso e infructuoso de entrar en la instalación, incluidos los casos en los que se concedió la admisión, debe registrarse de la siguiente manera:

- Fecha y hora
- Punto de entrada específico
- ID de usuario empleado durante el intento

Controles de construcción y seguridad interna

La construcción y la seguridad interna implican los bloqueos, llaves y requisitos de escolta/controles de visitantes que las organizaciones deben considerar. La construcción y la seguridad interna se tratan en detalle en el capítulo 3.

SEGURIDAD DEL PERSONAL

Los recursos humanos son los activos más importantes que posee la organización. Es posible recordar que en caso de incendio, la primera acción que siempre se debe tomar es evacuar a todo el personal. Su seguridad se produce antes que todas las demás consideraciones. Aunque el equipo y en la mayoría de los casos los datos pueden ser recuperados, los seres humanos no pueden ser respaldados ni reemplazados.

Un Plan de Emergencia de Ocupantes (OEP, por susatorias) proporciona procedimientos coordinados para minimizar la pérdida de vidas o lesiones y proteger los daños materiales en respuesta a una amenaza física. En un desastre de cualquier tipo, la seguridad del personal es la primera preocupación.

La organización es responsable de proteger la privacidad de la información de cada individuo, especialmente en lo que se refiere al personal y los registros médicos. Aunque esta expectativa de privacidad no se extiende necesariamente y por lo general no se extiende a sus actividades en la red, tanto las leyes federales como estatales responsabilizan a las organizaciones de la divulgación de este tipo de información, con violaciones que resultan en fuertes multas y posibles demandas si la compañía es encontrada responsable.

Las organizaciones deben desarrollar políticas para lidiar con la coacción de los empleados, los viajes, la supervisión, la gestión de emergencias y la capacitación y concienciación en seguridad.

coacción

La coacción de los empleados ocurre cuando un empleado es coaccionado para cometer una acción de otra parte. Esta es una preocupación particular para la administración de alto nivel o los empleados con autorizaciones de alta seguridad porque tienen acceso a activos adicionales. Las organizaciones deben capacitar a los empleados sobre qué hacer cuando están bajo coacción. Para los códigos de seguridad, PIN o contraseñas que se utilizan, es una buena política implementar un código de coacción secundario. Luego, si el personal está bajo coacción, utilizan el código de coacción para acceder a los sistemas, instalaciones u otros activos. Se alerta al personal de seguridad de que se ha utilizado el código de coacción. Las organizaciones deben hacer hincapié al personal en que la protección de la vida debe prevalecer sobre cualquier otra consideración.

viajar

Los empleados a menudo viajan con fines comerciales y toman sus activos emitidos por la organización mientras viajan. Los empleados deben recibir la capacitación adecuada para garantizar que mantienen seguros los activos emitidos por la organización durante el período de viaje y para tener especial cuidado cuando están en público. También deben recibir instrucciones sobre la notificación adecuada de los activos perdidos o robados.

monitorización

Es posible que sea necesario supervisar las acciones de los empleados sobre los activos organizativos, en particular para el personal con altos niveles de autorización. Sin embargo, es importante que el personal entienda que están siendo monitoreados. Las organizaciones que supervisarán a los empleados deben emitir una declaración sin expectativas de privacidad. Los empleados deben recibir una copia de este estado de cuenta cuando se contraten y deben firmar un recibo para el estado de cuenta. Además, los recordatorios periódicos de esta política deben colocarse en ubicaciones prominentes, incluidos los tablones de anuncios, las pantallas de inicio de sesión y los sitios web.

Para que cualquier supervisión sea efectiva, las organizaciones deben capturar el comportamiento de línea base para los usuarios.

Gestión de emergencias

Las organizaciones deben tener políticas y procedimientos específicos de manejo de emergencias. Los equipos de manejo de emergencias deben formarse para documentar los tipos de emergencias que podrían ocurrir y preparar los planes de emergencia apropiados que se utilizarán si se produce una emergencia específica.

Estos planes deben ser probados periódicamente para asegurar que el personal entienda qué hacer en caso de emergencia y revisado sobre la base de los resultados de estas pruebas.

Las emergencias que deben anticiparse incluyen eventos meteorológicos (como tornados, huracanes y tormentas invernales), situaciones de tiradores activos y cortes de energía. La gestión de emergencias a menudo conduce a la continuidad del negocio y la recuperación ante desastres si los efectos de la emergencia son a largo plazo. La gestión de emergencias se ocupa de la reacción inmediata a la emergencia. Si bien la continuidad del negocio y la recuperación ante desastres se centran en la recuperación de la organización a las operaciones normales, no todas las emergencias requerirán una recuperación completa ante desastres. Por ejemplo, si se notifica a una organización que se ha emitido una advertencia de tornado, la organización debe implementar el plan de emergencia para tornados. Si el tornado no afecta a la instalación, las operaciones pueden volver a la normalidad tan pronto como expire la advertencia. Sin embargo, si el tornado afecta a la instalación, podría ser necesario implementar los planes de continuidad del negocio y recuperación ante desastres.

Formación y sensibilización en seguridad

El personal debe recibir capacitación y conciencia de seguridad regularmente. La capacitación y la sensibilización en materia de seguridad se tratan en detalle en el capítulo 1.

TAREAS DE PREPARACIÓN DE EXÁMENES

Como se menciona en la sección"Acerca de la *Guía cissp cert,*tercera edición"en la introducción, usted tiene un par de opciones para la preparación del examen: los ejercicios aquí, capítulo 9,"Preparación final",y las preguntas de simulación de examen en el software pearson test prep en línea.

Revisar todos los temas clave

Revise los temas más importantes de este capítulo, que se indican con el icono Temas clave en el margen externo de la página. En la Tabla 7-2 se muestra una referencia de estos temas clave y los números de página en los que se encuentra cada uno.

Tabla 7-2 Temas clave para el Capítulo 7

Elemento clave del tema	descripción	Número de página
lista	Medidas de investigación forense	567
lista	Orden de volatilidad	569
lista	Principios de la IOCE	571
lista	Pasos de la escena del crimen	572
lista	Cinco reglas de evidencia	574
lista	Tipos de pruebas	575
lista	Tipos de análisis de medios	577
lista	Técnicas de análisis de software	578
lista	Técnicas de análisis de red	578
Figura 7-2	Proceso forense NIST SP 800-86	583
lista	Recomendaciones de NIST SP 800-86	584
sección	Tipos de registro	586
lista	Funciones de gestión de la configuración	592

Elemento clave del tema	descripción	Número de página
sección	Conceptos de operaciones de seguridad	593
Tabla 7-1	Niveles RAID	604
lista	Pasos de respuesta a incidentes	610
párrafo	Medidas de detective y preventivas	612
lista	Pasos del ciclo de vida de gestión de parches	617
lista	Tipos y esquemas de copia de seguridad de datos	624
Figure 7-12	Sitio caliente, sitio cálido y comparación de sitios fríos	629
lista	Tipos de pruebas utilizadas para evaluar el BCP y el DRP	638
sección	Controles de seguridad perimetral	640

Definir términos clave

Defina los siguientes términos clave de este capítulo y compruebe sus respuestas en el glosario:

sistemas acústicos

activo

mejor regla de evidencia

Listas negras

Bolardos

cadena de custodia

pruebas circunstanciales

investigación civil

Puerta de clase 1

Puerta de clase 2

Puerta de clase 3

Puerta de clase 4

niveles de recorte

sistema de televisión de circuito cerrado (CCTV)

sitio frío

pruebas concluyentes

análisis de contenido

copia de seguridad

pruebas corroborativas

escena del crimen

investigación criminal

copia de seguridad diaria

compensación de datos

software de prevención de pérdida de datos (DLP)

purga de datos

respaldo diferencial

pruebas directas

imágenes de disco

doble control

coacción

seguimiento de egresos

descubrimiento electrónico (exhibición electrónica)

bóveda electrónica

iluminación de emergencia

evento

conmutación por error

failsoft

tolerancia a fallos

pies de iluminación

primero en entrar, primero en salir (FIFO)

fluorescente

copia de seguridad completa

prueba de interrupción completa

abuelo/padre/hijo (GFS)

pruebas de rumores

sistema jerárquico de gestión del almacenamiento de información (HSM)

alta disponibilidad

honeynet

Honeypot

sitio caliente

incidente

copia de seguridad incremental

activos intangibles

rotación de puestos de trabajo

menor privilegio

medio

vapor de mercurio

motivo

iluminación móvil

necesidad de saber

almacenamiento conectado a la red (NAS)

investigación de operaciones

seguridad de las operaciones

pruebas de opinión

oportunidad

sistema infrarrojo pasivo (PIR)

sistema fotométrico

calidad del servicio (QoS)

lámpara de cuarzo

prueba paralela

RAID 0

RAID 1

RAID 2

RAID 3

RAID 5

RAID 10

prueba de lectura

acuerdo recíproco

redundancia

sitio redundante

investigación regulatoria

remanencia

aprovisionamiento de recursos

análisis de causa de raíz

sandboxing

buscar

pruebas secundarias

separación de funciones

acuerdo de nivel de servicio (SLA)

prueba de simulación

análisis de espacio flojo

vapor de sodio

iluminación en espera

análisis de esteganografía

red de área de almacenamiento (SAN)

prueba estructurada

vigilancia

resiliencia del sistema

activos tangibles

sitio terciario

copia de seguridad del registro de transacciones

ruta de confianza

recuperación de confianza

control de dos personas

sitio cálido

lista blanca

RESPONDER PREGUNTAS DE REVISIÓN

1 . ¿Cuál es el primer paso del proceso de respuesta a incidentes?

1. Responda al incidente.

2. Detecte el incidente.

3. Denuncie el incidente.

4. Recuperarse del incidente.

2 . ¿Cuál es el segundo paso del proceso de investigaciones forenses?

1. identificación

2. colección

3. preservación

4. examen

3 . ¿Cuál de las siguientes no es una de las cinco reglas de prueba?

1. Sé preciso.

2. Sé completo.

3. Sé admisible.

4. Sé volátil.

4 . ¿Cuál de las siguientes referencias se refiere a permitir a los usuarios acceder solo a los recursos necesarios para realizar su trabajo?

1. Rotación de empleo

2. Separación de funciones

3. Necesidad de saber/menos privilegios

4. Vacaciones obligatorias

5 . ¿Cuál de los siguientes es un ejemplo de un activo intangible?

1. Unidad de disco

2. receta

3. gente

4. servidor

6 . ¿Cuál de los siguientes no es un paso en la administración de respuesta a incidentes?

1. detectar

2. responder

3. monitor

4. informe

7 . ¿Cuál de los siguientes es NO es un tipo de copia de seguridad?

1. lleno

2. incremental

3. Abuelo/padre/hijo

4. Registro de transacciones

8 . ¿Qué término se utiliza para una instalación arrendada que contiene todos los recursos necesarios para su funcionamiento completo?

1. Sitio frío

2. Sitio caliente

3. Sitio cálido

4. Sitio terciario

9 . ¿Qué tipo de copia de seguridad electrónica almacena datos en discos ópticos y utiliza robótica para cargar y descargar los discos ópticos según sea necesario?

1. Máquina de discos óptica

2. Gestión jerárquica del almacenamiento

3. Bóveda de cinta

4. replicación

10. ¿Qué es failsoft?

1. La capacidad de un sistema para cambiar a un sistema de copia de seguridad si se produce un fallo en el sistema primario

2. La capacidad de un sistema para terminar procesos no críticos cuando se produce un error

3. Un producto de software que proporciona servicios de equilibrio de carga

4. Dispositivos de almacenamiento de alta capacidad conectados por una red privada de alta velocidad mediante conmutadores específicos del almacenamiento

11. ¿Qué tipo de investigación se refiere específicamente a litigios o investigaciones gubernamentales que se ocupan del intercambio de información en formato electrónico como parte del proceso de descubrimiento?

1. Prevención de pérdida de datos (DLP)

2. regulador

3. Exhibición electrónica

4. Operaciones

12. El firewall de una organización está supervisando el flujo de información saliente de una red a otra. ¿Qué tipo específico de monitoreo es este?

1. Seguimiento de egresos

2. Monitorización continua

3. CMaaS

4. Aprovisionamiento de recursos

13. ¿Cuál de los siguientes activos se considera activos virtuales? (Elija todo lo que corresponda.)

1. Redes definidas por software

2. Redes de área de almacenamiento virtual

3. Sistema operativo invitado implementado en máquinas virtuales

4. Routers virtuales

14. ¿Cuál de los siguientes describe la capacidad de un sistema, dispositivo o centro de datos para recuperarse rápidamente y continuar operando después de un fallo del equipo, apagón u otra interrupción?

1. Calidad del servicio (QoS)

2. Objetivo de tiempo de recuperación (RTO)

3. Objetivo de punto de recuperación (RPO)

4. Resiliencia del sistema

15. ¿Cuáles de los siguientes son los principales factores que afectan a la selección de una ubicación alternativa durante el desarrollo de un DRP? (Elija todo lo que corresponda.)

1. Ubicación geográfica

2. Necesidades organizativas

3. Costo de la ubicación

4. Esfuerzo de restauración de la ubicación

16. ¿Cuál de las siguientes opciones es una tecnología de disco duro en la que los datos se escriben en varios discos de tal manera que un disco puede fallar y los datos se pueden poner rápidamente a disposición de los discos restantes?

1. incursión

2. agrupamiento

3. Conmutación por error

4. Equilibrio de carga

17. Usted necesita registrar la información de tráfico de red entrante y saliente para determinar el origen de un ataque. ¿Qué registro de los siguientes registros debe usar?

1. Registro del sistema

2. Registro de aplicaciones

3. Registro de firewall

4. Cambiar registro

18. ¿Qué debe realizar en toda la información aceptada en un sistema para asegurarse de que es del tipo y formato de datos correctos y que no deja el sistema en un estado inseguro?

1. Niveles de recorte

2. Control de dos personas

3. Auditorías de revisión de acceso

4. Validación de entrada

19. ¿Cuál de las siguientes primeras líneas de defensa implementaría para desalentar a un intruso determinado?

1. Cerca de 3 a 4 pies de altura

2. Cerca de 6 a 7 pies de altura

3. 8 pies y cerca más alta

4. Geo-cerca

20. ¿Cuál de las siguientes acciones podría realizar para endurecer lógicamente un sistema? (Elija todo lo que corresponda.)

1. Elimine aplicaciones innecesarias.

2. Deshabilite servicios innecesarios.

3. Bloquear puertos no requisados.

4. Controle estrictamente la conexión de dispositivos y medios de almacenamiento externos.

RESPUESTAS Y EXPLICACIONES

1 . B. Los pasos del proceso de respuesta a incidentes son los siguientes:

1. Detecte el incidente.

2. Responda al incidente.

3. Informe del incidente al personal correspondiente.

4. Recuperarse del incidente.

5. Corrija todos los componentes afectados por el incidente para asegurarse de que se han eliminado todos los rastros del incidente.

6. Revise el incidente y documente todos los hallazgos.

2 . C. Los pasos del proceso de investigación forense son los siguientes:

1. identificación

2. preservación

3. colección

4. examen

5. análisis

6. presentación

7. decisión

3 . D. Las cinco normas de prueba son las siguientes:

- Sé auténtico.
- Sé preciso.
- Sé completo.
- Sé convincente.
- Sé admisible.

4 . C. Al permitir el acceso a los recursos y asignar derechos para realizar operaciones, siempre debe aplicarse el concepto de privilegios mínimos (también llamado necesidad de saber). En el contexto del acceso a recursos, esto significa que el nivel predeterminado de acceso no debe tener acceso. Dé a los usuarios acceso solamente a los recursos necesarios para hacer sus trabajos, y que el acceso debe requerir la implementación manual después de que un supervisor verifique el requisito.

5 . B. En muchos casos, algunos de los activos más valiosos para una empresa son intangibles, como recetas secretas, fórmulas y secretos comerciales.

6 . C. Los pasos en la administración de respuesta a incidentes son:

1. Detecte el incidente.

2. Responda al incidente.

3. Mitigar el incidente.

4. Denuncie el incidente.

5. Recuperarse del incidente.

6. Remediar el incidente.

7. Revisar y documentar las lecciones aprendidas.

7 . C. Abuelo/padre/hijo no es un tipo de respaldo; es un esquema de rotación de copia de seguridad.

8 . B. Un sitio caliente es una instalación arrendada que contiene todos los recursos necesarios para el funcionamiento completo.

9 . un. Una máquina de discos ópticos almacena datos en discos ópticos y utiliza robótica para cargar y descargar los discos ópticos según sea necesario.

10.b. Failsoft es la capacidad de un sistema para terminar procesos no críticos cuando se produce un error.

11.c. El descubrimiento electrónico (eDiscovery) se refiere a litigios o investigaciones gubernamentales que se ocupan del intercambio de información en formato electrónico como parte del proceso de descubrimiento. Implica información almacenada electrónicamente (ESI) e incluye correos electrónicos, documentos, presentaciones, bases de datos, correo de voz, archivos de audio y video, redes sociales y sitios web. El software de prevención de pérdida de datos (DLP) intenta evitar la fuga de datos. Lo hace manteniendo la conciencia de las acciones que se pueden y no se pueden tomar con respecto a un documento. Una investigación regulatoria

se produce cuando un organismo regulador investiga a una organización por una infracción reglamentaria. Las investigaciones de operaciones involucran cualquier investigación que no resulte en ningún asunto criminal, civil o regulatorio. En la mayoría de los casos, este tipo de investigación se completa para determinar la causa raíz para que se puedan tomar medidas para prevenir este incidente en el futuro.

12. a. La supervisión de salida se produce cuando una organización supervisa el flujo saliente de información de una red a otra. La forma más popular de monitoreo de salida se lleva a cabo utilizando firewalls que monitorean y controlan el tráfico saliente. La supervisión continua y la supervisión continua como servicio (CMaaS) no son lo suficientemente específicas como para responder a esta pregunta. Cualquier actividad de registro y supervisión debe formar parte de un programa de supervisión continua de la organización. El programa de supervisión continua debe diseñarse para satisfacer las necesidades de la organización e implementarse correctamente para garantizar que la infraestructura crítica de la organización esté protegida. Es posible que las organizaciones quieran examinar las soluciones de CMaaS implementadas por los proveedores de servicios en la nube. El aprovisionamiento de recursos es el proceso en las operaciones de seguridad que garantiza que la organización solo implemente los activos que necesita actualmente.

13. a, b, c, d. Los activos virtuales incluyen redes definidas por software (SDN), redes de área de almacenamiento virtual (VSAN), sistemas operativos invitados implementados en máquinas virtuales (VM) y enrutadores virtuales. Al igual que con los activos físicos, la implementación y el desmantelamiento de activos virtuales deben controlarse estrictamente como parte de la administración de la configuración porque los activos virtuales, como los activos físicos, pueden verse comprometidos.

14. d. La resiliencia del sistema es la capacidad de un sistema, dispositivo o centro de datos para recuperarse rápidamente y continuar operando después de un fallo del equipo, apagón u otra interrupción. Implica el uso de componentes o instalaciones redundantes. La calidad del servicio (QoS) es una tecnología que administra los recursos de red para garantizar un nivel de servicio predefinido. Asigna las prioridades de tráfico a los diversos tipos de tráfico en una red. Un objetivo de tiempo de recuperación (RTO) estipula la cantidad de tiempo que una organización necesita para recuperarse de un desastre, y un objetivo de punto de recuperación (RPO) estipula la cantidad de datos que una organización puede perder cuando se produce un desastre.

15.a, b, c, d. Los principales factores que afectan a la selección de una ubicación alternativa durante el desarrollo de un plan de recuperación ante desastres (DRP) incluyen los siguientes:

- Ubicación geográfica
- Necesidades organizativas

- Costo de la ubicación
- Esfuerzo de restauración de la ubicación

16. a. Redundant Array of Independent Disks (RAID) es una tecnología de disco duro en la que los datos se escriben en varios discos de tal manera que un disco puede fallar y los datos se pueden hacer disponibles rápidamente desde los discos restantes de la matriz sin restaurarlos desde una cinta de copia de seguridad u otros medios de copia de seguridad. Clustering hace referencia a un producto de software que proporciona servicios de equilibrio de carga. Con la agrupación en clústeres, una instancia de un servidor de aplicaciones actúa como controlador maestro y distribuye solicitudes a varias instancias mediante algoritmos round robin, round robin ponderado o de conexiones de menor. La conmutación por error es la capacidad de un sistema para cambiar a un sistema de copia de seguridad si se produce un error en el sistema primario. El equilibrio de carga se refiere a un producto de hardware que proporciona servicios de equilibrio de carga. Los controladores de entrega de aplicaciones (ADC) admiten los mismos algoritmos, pero también utilizan procesos complejos de contracción de números, como cpu por servidor y utilización de memoria, tiempos de respuesta más rápidos, etc., para ajustar el equilibrio de la carga. Las soluciones de equilibrio de carga también se conocen como granjas de servidores o grupos.

17.c. Los registros de firewall registran la información de tráfico de red, incluido el tráfico entrante y saliente. Esto normalmente incluye datos importantes, como direcciones IP y números de puerto que se pueden usar para determinar el origen de un ataque. Los registros del sistema registran eventos del sistema, como el inicio y apagado del sistema y del servicio. Las aplicaciones registran las acciones de registro que se producen dentro de una aplicación específica. Los cambios en los registros informan de los cambios realizados en un dispositivo o aplicación específico como parte del proceso de administración de cambios.

18. d. El principal impulso del control de entrada/salida es aplicar controles o comprobaciones a la entrada que se permite enviar al sistema. Realizar la validación de entrada en toda la información aceptada en el sistema puede garantizar que es del tipo y formato de datos correctos y que no deja el sistema en un estado inseguro. Los niveles de recorte establecen una línea base para los errores normales del usuario y se registrarán infracciones que superen ese umbral para analizar por qué se produjeron las infracciones. Un control de dos personas, también conocido como regla de dos hombres, ocurre cuando ciertos accesos y acciones requieren la presencia de dos personas autorizadas en todo momento. Las auditorías de revisión de acceso garantizan que el acceso a objetos y las prácticas de administración de cuentas de usuario se adhieran a la directiva de seguridad de la organización.

19.c. La esgrima es la primera línea de defensa en el paradigma del círculo concéntrico. Al seleccionar el tipo de cerca para instalar, considere la

determinación de la persona que está tratando de desalentar. Utilice las siguientes directrices con respecto a la altura:

- Las vallas de 3 a 4 pies de altura disuaden sólo a los intrusos casuales.
- Las vallas de 6 a 7 pies de altura son demasiado altas para escalar fácilmente.
- Vallas de 8 pies y disuasión más alta intrusos más determinados, especialmente cuando se aumenta con alambre de afeitar.

Una geo-cerca es un área geográfica dentro de la cual los dispositivos se gestionan utilizando algún tipo de comunicación de radiofrecuencia. Se utiliza para rastrear a los usuarios o dispositivos que entran o salen del área de geo-cerca.

20.a, b, c, d. Un objetivo continuo de la seguridad de las operaciones es garantizar que todos los sistemas se hayan endurecido en la medida en que sea posible y sigan proporcionando funcionalidad. Se pueden realizar las siguientes acciones para endurecer lógicamente un sistema:

- Elimine aplicaciones innecesarias.
- Deshabilite servicios innecesarios.
- Bloquear puertos no requisados.
- Controle estrictamente la conexión de dispositivos de almacenamiento externos y medios si está permitido en absoluto.