Capítulo 7: Operaciones de seguridad

En este capítulo se tratan los siguientes temas:

- **Investigaciones:** Los conceptos discutidos incluyen investigaciones y procedimientos forenses y digitales, informes y documentación, técnicas de investigación, recopilación y manejo de evidencia, y herramientas, tácticas y procedimientos forenses digitales.
- **Tipos de investigación:** Los conceptos analizados incluyen operaciones/investigaciones administrativas, penales, civiles, reglamentarias, de la industria y 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 administración de eventos, monitoreo continuo y monitoreo de salida.
- **Aprovisionamiento de recursos:** Los conceptos descritos incluyen el inventario y la administración de activos, la administración de la configuración, los activos físicos, los activos virtuales, los activos en la nube y las aplicaciones.
- **Conceptos de operaciones de seguridad:** Los conceptos discutidos incluyen necesidad de saber/privilegios mínimos; administrar cuentas, grupos y roles; separación de funciones y responsabilidades; administración de cuentas privilegiadas; rotación de puestos de trabajo y vacaciones obligatorias; control de dos personas; procedimientos de información sensible; 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 administración de activos de medios, hardware y software.
- **Gestión de incidentes:** Los conceptos discutidos incluyen eventos versus incidentes, equipo de respuesta a incidentes e investigaciones de incidentes, reglas de compromiso, autorización, alcance, procedimientos de respuesta a incidentes, administración de respuesta a incidentes y los pasos en el proceso de respuesta a incidentes.
- **Medidas detectivescas y preventivas:** Los conceptos discutidos incluyen IDS/IPS, firewalls, listas blancas/listas negras, servicios de seguridad de terceros, sandboxing, honeypots/honeynets, antimalware/antivirus, niveles de recorte, desviaciones de estándares, eventos inusuales o inexplicables, reinicios no programados, divulgación no autorizada, recuperación confiable, rutas de confianza, controles de entrada/salida, endurecimiento del sistema y sistemas de gestión de vulnerabilidades.
- **Gestión de parches y vulnerabilidades:** Entre los conceptos descritos se incluye 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 estrategias de múltiples sitios; sistemas, instalaciones y energía redundantes; tecnologías de tolerancia a fallos; seguros; 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 concientización.
- **Probar planes de recuperación ante desastres:** Los conceptos discutidos incluyen prueba de lectura, prueba de lista de verificación, ejercicio de mesa, prueba de recorrido estructurado, prueba de simulación, prueba paralela, prueba de interrupción completa, perforación funcional y taladro de evacuación.
- **Planificación y ejercicios de continuidad del negocio:** Los conceptos discutidos incluyen la planificación de la continuidad del negocio y los ejercicios.
- **Seguridad física:** Los conceptos discutidos incluyen controles de seguridad perimetral y controles de seguridad interna.
- **Seguridad y protección del personal:** Los conceptos discutidos incluyen coacción, viajes, monitoreo, manejo de emergencias y capacitación y concientización en seguridad.

Las operaciones de seguridad incluyen conceptos fundamentales de operaciones de seguridad, investigaciones, administración de incidentes y recuperación ante desastres. También cubre la seguridad física y del personal. Los profesionales de la seguridad deben recibir la capacitación adecuada en estas áreas o emplear a 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 que incluyen investigaciones, registro, supervisión, aprovisionamiento, conceptos de operaciones de seguridad, protección de recursos, administración de incidentes, medidas preventivas y de detectives, 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 empatado con otros dos dominios. Por lo tanto, ¡preste 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 manera segura. Se ocupa de investigar, gestionar y prevenir eventos o incidentes. También cubre el registro de actividades 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 provisión de seguridad física. Las operaciones de seguridad implican el funcionamiento diario de una organización.

Table of Contents

7.1 Investigaciones

Las investigaciones deben llevarse a cabo de la manera adecuada para garantizar que las pruebas reunidas puedan utilizarse en los tribunales. Sin las investigaciones adecuadas y la recopilación de pruebas, los atacantes no serán responsables de sus acciones. En esta sección discutimos las 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 se comprime y se puede requerir un experto 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. Finalmente, la evidencia en un delito informático es mucho más difícil de reunir.

Después de que se haya tomado la decisión de investigar un delito informático, debe seguir 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 la evidencia.

Después de que la policía ha sido informada de un delito informático, las limitaciones del investigador de la organización se incrementan. Podría ser necesario entregar la investigación a las fuerzas del orden para garantizar que las pruebas se conserven adecuadamente.

Al investigar un delito informático, se deben abordar las normas probatorias. La evidencia informática debe probar un hecho que sea 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 la corte como evidencia si el proceso para producirla no ha sido documentado.

Nota

Si bien la mayor parte de la discusión de las investigaciones se centra en las 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 deseen supervisar al personal para asegurarse de que no se infringe la directiva de uso aceptable (AUP). Los profesionales de la seguridad deben asegurarse de que estas investigaciones se coordinen para incluir al personal de recursos humanos. Las investigaciones internas a menudo pueden ser tan importantes como las investigaciones criminales.

PuntoClave1:

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.

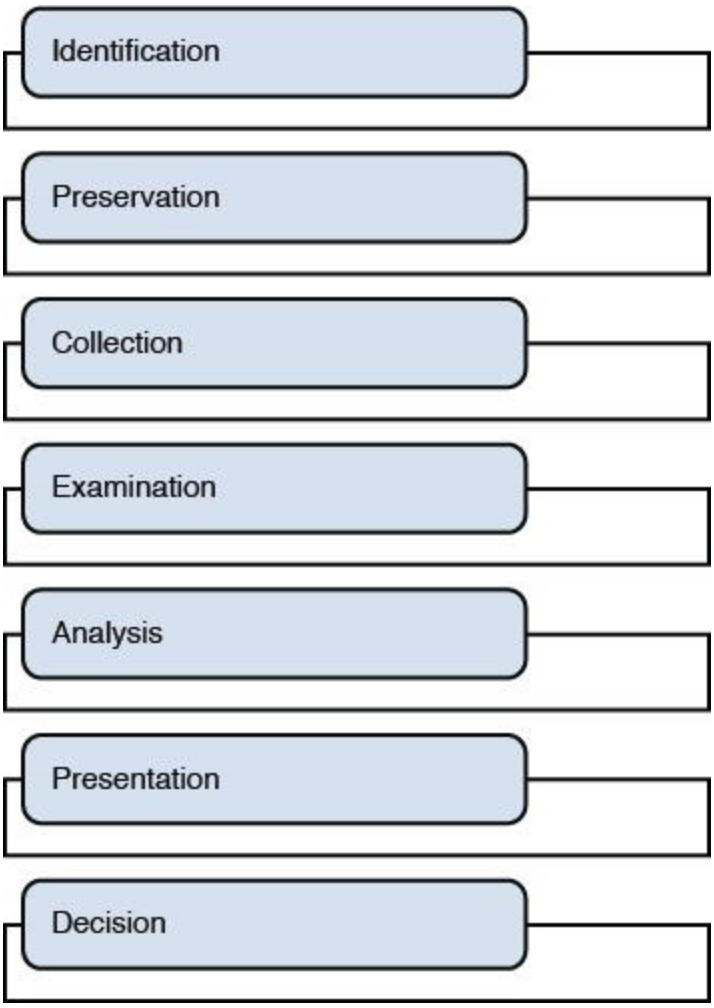


Figura 7-1 Proceso de Investigación Forense

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

Identificar evidencia

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 a través de la revisión de registros de auditoría, el monitoreo de sistemas, el análisis de quejas de usuarios y el análisis de mecanismos de detección. Inicialmente, los investigadores podrían no estar seguros de qué evidencia es importante. Preservar la evidencia que tal vez no necesite siempre es mejor que desear tener evidencia que no retuvo.

La identificación de 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

desde el que se originó el ataque también puede considerarse parte de la escena del crimen. Sin embargo, la captura completa de los sistemas del atacante no siempre es posible. Por este motivo, debe asegurarse de capturar los datos que puedan apuntar a un sistema específico, como la captura de direcciones IP, nombres de usuario y otros identificadores.

Preservar y recopilar pruebas

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

Antes de recopilar cualquier evidencia, considere el orden de volatilidad. Esta orden garantiza que los investigadores recopilen evidencia de los componentes que son más volátiles primero.

PuntoClave2

El orden de volatilidad es el siguiente:

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

Para crear imágenes del sistema, debe utilizar una herramienta que cree una copia a nivel de bits del sistema. En la mayoría de los casos, debe aislar el sistema y quitarlo 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 no dañada esté disponible como evidencia. La otra copia se utilizará durante los pasos de examen y análisis. Los resúmenes de mensajes deben utilizarse para garantizar la integridad de los datos.

Aunque la imagen del sistema suele ser la pieza de evidencia más importante, no es la única evidencia que necesita. Es posible que también necesite capturar datos almacenados en la memoria caché, las tablas de proceso, la memoria y el Registro. Al documentar un ataque informático, debe utilizar un bloc de notas enlazado para mantener notas.

Recuerde que podría ser necesario recurrir a expertos en investigaciones digitales para garantizar que las pruebas se conserven y recopilen adecuadamente. Los investigadores

ensamblan generalmente un kit de campo para ayudar en el proceso de investigación. Este kit puede incluir etiquetas y etiquetas, herramientas de desmontaje y embalaje a prueba de manipulaciones. Los kits de campo comerciales están disponibles, o podría ensamblar los suyos propios en función de las necesidades de la organización.

Examinar y analizar la evidencia

Después de que la evidencia ha sido preservada y recolectada, el investigador necesita examinar y analizar la evidencia. Al examinar la evidencia, se debe determinar y documentar cualquier característica, como las marcas de tiempo y las propiedades de identificación. Después de que la evidencia haya sido completamente analizada utilizando métodos científicos, el incidente completo debe ser reconstruido y documentado.

Conclusiones actuales

Después de un examen y análisis de las pruebas, deben presentarse como prueba en el tribunal. En la mayoría de los casos, cuando se presentan pruebas en la corte, la presentación de los hallazgos en un formato que la audiencia puede entender es mejor. Aunque se debe utilizar a un experto para testificar sobre los hallazgos, es importante que el experto pueda articular a una audiencia no técnica los detalles de la evidencia.

Decidir

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

Procedimientos forenses

La recopilación de evidencia digital es más complicada que la recopilación de evidencia física 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 de justicia. Es responsabilidad de la persona capacitada asegurarse de que los procedimientos que utilizan siguen las normas establecidas. Organizaciones como el Instituto Nacional de Normas y Tecnología (NIST) y la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional (ISO/IEC), establecen normas que ayudan a orientar a las organizaciones en el establecimiento adecuado de estos y otros procedimientos. Siempre consulte con estos

estándares antes de realizar cualquier investigación para determinar si los procedimientos sugeridos han cambiado o si hay nuevas herramientas disponibles.

Presentación de informes y documentación

Una vez finalizada cualquier investigación, los profesionales de la seguridad deben proporcionar informes y documentación a la administración con respecto al incidente. Este informe debe presentarse a la administración lo antes posible para que la administración pueda determinar si es necesario implementar controles para prevenir el incidente. Esta presentación a la gerencia a menudo ocurrirá antes de la presentación de cualquier conclusión legal en un tribunal de justicia. Las organizaciones deben establecer procedimientos para garantizar que las personas a las que se presentan los informes tengan la autorización adecuada. También puede ser necesario redactar ciertas partes del informe para garantizar que las causas penales no se vean afectadas negativamente.

Si bien los informes internos son importantes, los profesionales de la seguridad también deben tener directrices sobre cuándo denunciar los incidentes a las fuerzas del orden. Cuanto antes esté involucrada la aplicación de la ley, más probable es que las pruebas sean admisibles en un tribunal de justicia. Sin embargo, la mayoría de las fuerzas del orden locales no tienen el conocimiento o las 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 que realice la investigación. También se debe traer a profesionales del derecho para que ayuden.

La documentación adecuada debe mantenerse durante toda 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 estándares para las investigaciones digitales. Ambos grupos publican directrices sobre muchos formatos de información digital, incluidos los datos informáticos, los datos de dispositivos móviles, los datos de sistemas informáticos de automóviles, etc. Cualquier investigador debe asegurarse de que cumple con los principios de estos grupos.

PuntoClave3

Si bien el IOCE ya no es un organismo de evidencia en funcionamiento, sí estableció algunos principios que todavía son aplicables hoy en día. Los principios fundamentales documentados por IOCE son los siguientes:

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

NIST SP 800-86, "Guía para integrar técnicas forenses en la respuesta a incidentes", proporciona directrices sobre la recopilación de datos, el examen, el análisis y la presentación de informes relacionados con la ciencia forense digital. 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 a cualquier investigación forense.

Nota

NIST SP 800-86 se discute con más detalle más adelante en la sección " Estándares de la Industria" de este capítulo.

Escena del crimen

Una escena del crimen es el entorno en el que existen pruebas potenciales. Una vez identificado el lugar del delito, deben adoptarse medidas para garantizar la protección del medio ambiente, incluidos el entorno físico y virtual. Para asegurar la escena física del crimen, un investigador podría necesitar aislar los sistemas involucrados eliminándolos de una red. Sin embargo, los sistemas NO deben apagarse hasta que el investigador esté seguro de que se ha capturado toda la evidencia digital. Recuerde: Los datos de la computadora en vivo son dinámicos y posiblemente se almacenan en varias ubicaciones volátiles.

PuntoClave4

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

1. Identificar la escena del crimen.
2. Proteger toda la escena del crimen.
3. Identificar cualquier pieza de evidencia o fuentes potenciales de evidencia que formen parte de la escena del crimen.
4. Recoger todas las pruebas en la escena del crimen.
5. Minimice la contaminación asegurando y preservando adecuadamente toda la evidencia.

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

El acceso a la escena del crimen debe estar estrictamente controlado y limitado sólo a las personas 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 ninguna manera de restaurarla a la condición original.

MOM

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

Comprender MOM puede ayudar a cualquier investigador a reducir la lista de sospechosos.

Cadena de custodia

Al comienzo de cualquier investigación, debe hacer las preguntas sobre 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 la evidencia, quién aseguró la evidencia y quién la obtuvo. 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 reglamentos.

Los formularios de cadena de custodia deben usarse para rastrear quién tiene acceso a la evidencia, cuándo se produce ese acceso y otros detalles valiosos basados en las necesidades de la organización o la investigación. Este formulario de 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 sean admisibles en los tribunales. Los oficiales de la aplicación de ley acentúan la cadena de la custodia en cualquier investigación que conduzcan. Involucrar a la policía 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 la evidencia necesita ser obtenida, asegurarse de que el entrevistador entienda qué información necesita ser obtenida y todas las preguntas a cubrir es importante. Leer a un sospechoso sus derechos SÓLO es necesario si la policía está realizando la entrevista. La grabación de 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 participar en cualquier interrogatorio del sospechoso. El empleado sólo debe ser entrevistado por una persona que es mayor a ese empleado.

Técnicas de investigación

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

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

Una vez que se completen las entrevistas y la vigilancia reúna suficiente evidencia, los investigadores querrán realizar análisis forenses avanzados. Las organizaciones pueden hacer esto monitoreando continuamente la actividad, pero si la policía está involucrada, se deberá obtener una orden judicial que permita el análisis forense de las 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 delitos pueden requerir que los investigadores vayan encubiertos, adoptando personajes falsos en línea para atrapar a los 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.

Recopilación y manejo de evidencias

Para que las pruebas sean admisibles, deben ser pertinentes, legalmente permisibles, fiables, debidamente identificadas y debidamente conservadas. *Relevante* significa que debe probar un hecho material relacionado con el crimen en el sentido de que demuestra que se ha cometido un delito, puede proporcionar información que describe el delito, puede proporcionar información sobre los motivos del perpetrador o puede verificar lo que ocurrió. *Legalmente permisible* significa que la evidencia es considerada por el juez como útil para ayudar al jurado o juez a llegar a una decisión y no puede ser objetada sobre la base de que es irrelevante, inmaterial o viola las reglas contra rumores y otras objeciones. *La confiabilidad* significa que no ha sido manipulado o modificado. *Correctamente identificado* significa que la evidencia se etiqueta apropiadamente y se introduce en el registro de evidencia. *La preservación* significa que las pruebas no están sujetas a daños o destrucción.

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

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

Cinco reglas de evidencia

PuntoClave5

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

- Sé auténtico.
- Sea preciso.
- Sé completo.
- Sea convincente.

- Ser 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 ser consciente de los tipos de evidencia utilizados en la corte para asegurarse de que todas las pruebas son admisibles. A veces el tipo de evidencia determina su admisibilidad.

PuntoClave6

Los tipos de evidencia que debe comprender son los siguientes:

- La mejor evidencia
- Evidencia secundaria
- Pruebas directas
- Pruebas concluyentes
- Evidencia circunstancial
- Pruebas corroborativas
- Evidencia de opinión
- Pruebas de oídas

Mejor evidencia

La regla de la mejor evidencia establece que cuando se presentan pruebas, como un documento o una grabación, solo se aceptará el original a menos que exista una razón legítima de por qué no se puede usar 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 regla de la mejor evidencia a la evidencia digital caso por caso, dependiendo de la evidencia y la situación. En esta situación, la copia debe ser probada por un testigo experto que pueda testificar sobre el contenido y confirmar que es una copia exacta del original.

Evidencia secundaria

Las pruebas secundarias se han reproducido a partir de un artículo original o se han sustituido por un artículo original. Las copias de los documentos originales y los testimonios orales se consideran pruebas secundarias.

Evidencia directa

La evidencia directa prueba o refuta un hecho a través de testimonios orales basados en información recopilada a través de los sentidos del testigo. Un testigo puede testificar sobre lo que vio, olió, oyó, probó o sintió. Esto se considera evidencia directa. Sólo el testigo puede declarar directamente. Nadie más puede informar sobre lo que el testigo les dijo porque eso se considera evidencia de oídas.

Pruebas concluyentes

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

Evidencia circunstancial

La evidencia circunstancial proporciona inferencia de información de otros hechos relevantes intermedios. Esta evidencia ayuda a un jurado a llegar a una conclusión al usar un hecho para dar a entender que otro hecho es verdadero o falso. Un ejemplo es dar a entender que un ex empleado cometió un acto contra una organización debido a su aversión a la organización después de su despido.

Evidencia corroborativa

La evidencia corroborativa apoya otra pieza de evidencia. Por ejemplo, si un sospechoso presenta 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 que lo corroboran a través de su testimonio.

Evidencia de opinión

La evidencia de opinión se basa en lo que el testigo piensa, siente o infiere con respecto a los hechos. Sin embargo, si se utiliza un testigo experto, ese experto puede testificar sobre un hecho basado en su conocimiento en un área determinada. Por ejemplo, un psiquiatra puede testificar sobre las conclusiones sobre el estado de ánimo de un sospechoso. El testimonio de un experto no se considera evidencia de opinión debido al conocimiento y la experiencia del experto.

Pruebas de oídas

La evidencia de oídas es una evidencia que es de segunda mano, donde el testigo no tiene conocimiento directo del hecho afirmado, sino que lo conoce solo a partir de alguien que alguien le ha dicho. En algunos casos, la evidencia basada en computadoras se considera de oídas, especialmente si un experto no puede testificar sobre la exactitud e integridad de la evidencia.

Vigilancia, registro e incautación

La vigilancia, el registro 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.

Los investigadores utilizan dos tipos de vigilancia: la vigilancia física y la vigilancia informática. La vigilancia física ocurre cuando las acciones de una persona son reportadas o capturadas usando cámaras, observancia directa o circuito cerrado de TV (CCTV). La vigilancia informática se produce cuando las acciones de una persona se notifican o capturan utilizando información digital, como registros de auditoría.

En la mayoría de los casos se requiere una orden de registro para buscar activamente pruebas en un sitio privado. Para que se emita una orden de registro, la causa probable de que se haya cometido un delito debe probarse ante un juez. El juez también debe ser corroborado sobre la existencia de pruebas. La única vez que no es necesario emitir una orden de registro es durante circunstancias extremas, que son circunstancias de emergencia que son necesarias para evitar daños físicos, la destrucción de pruebas, la fuga del sospechoso o alguna otra consecuencia que frustró indebidamente los esfuerzos legítimos de aplicación de la ley. Las circunstancias extremas tendrán que ser probadas cuando las pruebas se presenten en el tribunal.

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. Las pruebas enumeradas específicamente en la orden de registro pueden ser incautadas, y el registro solo puede ocurrir en áreas específicamente enumeradas en la orden.

Las reglas de registro e incautación no se aplican a organizaciones privadas ni a 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.

Un análisis de las pruebas estaría incompleto sin examinar la jurisdicción. Debido a que los delitos informáticos pueden involucrar 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 local encargado de hacer cumplir la ley para cualquier investigación penal o civil y seguir cualquier consejo que den para las investigaciones que cruzan las 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.

PuntoClave7

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 de holgura (marcado como vacío o reutilizable) en la unidad para ver si se puede recuperar algún dato antiguo (marcado 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 se han modificado o para descubrir 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 máquina. A menudo implica descompilar o ingeniería inversa. Este tipo de análisis se utiliza a menudo durante el análisis de malware y disputas de derechos de autor.

PuntoClave8

Las técnicas de análisis de software incluyen lo siguiente:

- **Análisis de contenido:** Analiza el contenido del software, en particular el malware, para determinar para qué propósito se creó el software.
- **Ingeniería inversa:** Recupera el código fuente de un programa para estudiar cómo el programa realiza 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 preservar los registros y la actividad como evidencia.

PuntoClave9

Las técnicas de análisis de red incluyen lo siguiente:

- **Análisis de comunicaciones:** Analiza la comunicación a través de una red capturando toda o parte de la comunicación y buscando determinados tipos de actividad.
- **Análisis de registros:** Analiza los registros de tráfico de red.
- **Seguimiento de la ruta de acceso:** Realiza un seguimiento de la ruta de acceso de un paquete de tráfico determinado o un tipo de tráfico para detectar la ruta utilizada por el atacante.

Análisis de hardware/dispositivos integrados

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 del dispositivo puede proporcionar asesoramiento sobre la mejor técnica para usar en función 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 dispositivos móviles. Para realizar este tipo de análisis, el NIST hace las siguientes recomendaciones:

- Cualquier análisis no debe cambiar los datos contenidos en el dispositivo o medio.
- Sólo los investigadores competentes deben acceder a los datos originales y deben explicar todas las acciones que tomaron.
- Las pistas 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 relacionadas con la evidencia digital, incluida su incautación, acceso a ella, su almacenamiento o su transferencia, deben documentarse, preservarse y estar disponibles para su revisión.

Herramientas, tácticas y procedimientos forenses digitales

Para la recopilación de pruebas, los investigadores necesitarán un conjunto de herramientas digitales. Lo siguiente debe incluirse como parte de cualquier conjunto de herramientas digitales:

- Computadoras portátiles forenses y fuentes de alimentación
- Conjuntos de herramientas
- Cámara digital
- Carpeta de casos
- Formularios en blanco
- Recogida de pruebas y suministros de embalaje
- Software
- Tarjeta de aire 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 conjunto de herramientas digitales debe contener herramientas forenses que permitan a un investigador obtener datos que puedan utilizarse como prueba. 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 datos y discos
- Visores de archivos
- Herramientas de análisis de archivos
- Herramientas de análisis del Registro
- 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 red
- Herramientas forenses de base de datos

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

Entre las herramientas que se pueden incluir en un kit de herramientas forense digital se incluyen las siguientes:

- Marco forense digital (DFF)
- Arquitectura forense de computadora abierta (OCFA)
- Entorno INvestigativo Asistido por Ordenador (CAINE)
- Forense de X-Ways
- Kit de herramientas forenses de investigación de SANS (SIFT)
- EnCase Forense
- Reconocimiento del registro
- El kit de Sleuth (TSK)
- LibForensics

- Volatilidad
- Ámbito de Windows
- El kit de herramientas del forense (TCT)
- Suite forense de oxígeno
- Bulk_Extractor
- Xplico
- Redline
- Extractor de evidencia forense en línea por computadora (COFEE)
- PlainSight
- 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 garantizar que se sigan las herramientas, tácticas y procedimientos para que las pruebas recopiladas sean admisibles en los tribunales. Tenga en cuenta que 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 comprender que estas herramientas, tácticas y procedimientos proporcionan automatización de la investigación forense digital y cumplimiento de los estándares de investigación. El rol de trabajo de un candidato CISSP no se define como la realización de tareas individuales de investigación forense; sin embargo, el profesional de 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.

7.2 Tipos de investigación

Se llama a los profesionales de la seguridad para que investiguen cualquier incidente que ocurra. Como resultado de los diferentes activos que se ven afectados, los profesionales de la seguridad deben poder realizar diferentes tipos de investigaciones, incluidas las investigaciones de operaciones/administrativas, penales, civiles, reglamentarias, estándar de la industria y de exhibición de documentos electrónicos. Estos tipos de investigación se describen en las secciones siguientes.

Operaciones/Administrativas

Las investigaciones administrativas son investigaciones que no resultan en ningún problema penal, civil o regulatorio. 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, de modo que se puedan tomar medidas para evitar que este incidente vuelva a ocurrir en el futuro. Este proceso se conoce

como *análisis de causa de origen.* Debido a que no se ha violado ninguna ley penal, civil o regulatoria, no es tan importante documentar la evidencia. Sin embargo, los profesionales de la seguridad aún deben tomar medidas para documentar las lecciones aprendidas.

Como ejemplo de este tipo de investigación, supongamos que a un usuario se le asignan permisos inadecuados en función de su rol de trabajo. Si esto es el resultado de una acción criminal, debe producirse una investigación penal. 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 pautas. Cualquier persona que lleve a cabo este tipo de investigación debe asegurarse de que se realizan los cambios apropiados 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 inadecuados, el profesional de la 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 la policía esté involucrada 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 que otra organización está incurriendo en actos ilícitos 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, solo pueden ser presentados por fiscales del gobierno. En un caso civil, la organización debe asegurarse de que se sigan todas las reglas de evidencia y que la representación legal esté involucrada como parte de la investigación.

Regulador

Una investigación regulatoria ocurre cuando un organismo regulador investiga a una organización por una infracción regulatoria. En la historia reciente, la Comisión de Bolsa y Valores (SEC) ha llevado a cabo muchas investigaciones regulatorias con respecto a las organizaciones y sus transacciones financieras. Independientemente del organismo regulador que esté llevando a cabo la investigación, se notificará a la organización investigada 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 la presentación de cargos contra la organización y cualquier personal involucrado.

Estándares de la industria

Como se definió en capítulos anteriores, las normas proporcionan criterios dentro de una industria relacionados con el funcionamiento estándar y la realización de operaciones en sus respectivos campos de producción. En forense digital, los estándares proporcionan los requisitos generalmente aceptados seguidos por los investigadores digitales.

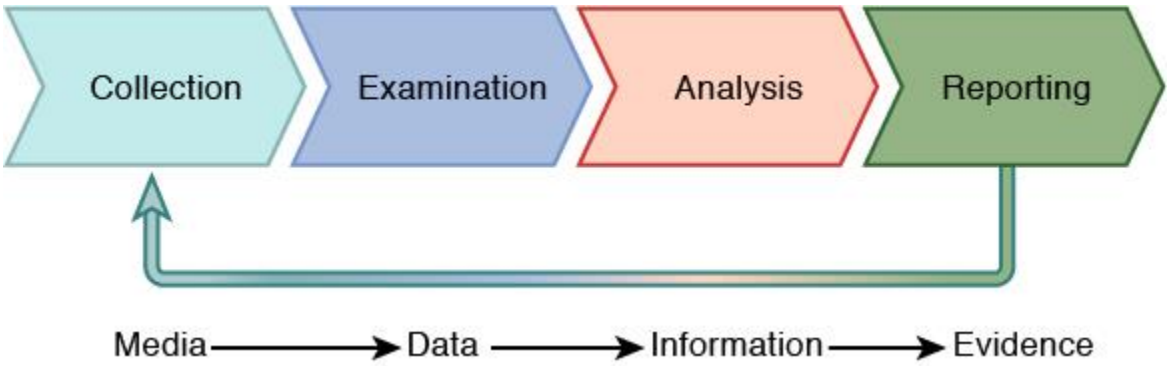
Las organizaciones deben investigar los estándares forenses digitales disponibles, incluidos los del NIST y la ISO/IEC. NIST SP 800-86 proporciona directrices para integrar técnicas forenses en la respuesta a incidentes.

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

- Las organizaciones deben tener la capacidad de realizar análisis forenses informáticos y de red.
- Las organizaciones deben determinar qué partes deben manejar cada aspecto de la medicina forense.
- Los equipos de manejo de incidentes deben tener capacidades forenses sólidas.
- Muchos equipos dentro de una organización deben participar en la medicina forense.
- 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, examen, análisis y presentación de informes. Esto difiere ligeramente del proceso reportado anteriormente. En algunos casos, los dos primeros pasos presentados anteriormente (identificación y preservación) se consideran parte de la respuesta al incidente, pero no parte del proceso forense en sí. Sin embargo, las cuatro fases de 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, ya sea que se necesite evidencia para la aplicación de la ley o para el uso interno de una organización.

PuntoClave10



El proceso forense se procesa en las siguientes fases: Recopilación, Examen, Análisis e Informes. Flecha desde los puntos de notificación hasta la colección. A continuación, los medios fluyen a los datos que fluyen a la información y finalmente conducen a la evidencia.

Figura 7-2 Proceso forense NIST SP 800-86 (imagen cortesía del NIST)

Durante la recopilación, los datos relacionados con un evento específico se identifican, etiquetan, registran y recopilan, y se preserva su integridad. En la segunda fase, se ejecutan herramientas de examen, herramientas forenses y técnicas adecuadas a los tipos de datos que se recopilaron para identificar y extraer la información relevante de los datos recopilados, protegiendo al mismo tiempo 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 derivar información útil que aborde las preguntas que fueron el impulso para realizar la recopilación y el examen. La fase final implica informar 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 a las políticas, directrices, procedimientos, herramientas y otros aspectos del proceso forense.

PuntoClave11

Las principales recomendaciones para el proceso forense son las siguientes:

- Las organizaciones deben realizar análisis forenses utilizando 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 el uso de datos de archivos de datos son las siguientes:

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

Las recomendaciones clave presentadas para el uso de datos de los sistemas operativos son las siguientes:

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

Las recomendaciones clave presentadas para usar los 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 un conocimiento técnico razonablemente completo.
- Los analistas deben tener en cuenta la fidelidad y el valor de cada origen de datos.
- Los analistas generalmente 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 tener en cuenta todos los posibles orígenes de datos de aplicación.
- 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 controlar muchas situaciones de forma más eficaz analizando varios orígenes de datos individuales y, a continuación, correlacionando eventos entre ellos.

- Las organizaciones deben ser conscientes de la complejidad técnica y logística del análisis.

Exhibición de documentos electrónicos

*El descubrimiento electrónico (eDiscovery)*se refiere a litigios o investigaciones gubernamentales que tratan con el intercambio de información en formato electrónico como parte del proceso de descubrimiento. Involucra 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 expolio o manipulación de pruebas más adelante en el litigio. Una vez que se recopila la ESI adecuada, debe mantenerse en un entorno seguro para su revisión.

7.3 Actividades de registro y supervisión

Como parte de la seguridad de las operaciones, los administradores deben asegurarse de que las actividades de los usuarios se registran y supervisan regularmente. Esto incluye auditoría y revisión, detección y prevención de intrusiones, información de seguridad y gestión de eventos, supervisión continua y supervisión de salida.

Auditoría y revisión

La rendición de cuentas es imposible sin un registro de las actividades y un examen de esas actividades. La captura y supervisión de registros de auditoría proporciona la prueba digital cuando es necesario identificar a alguien que está realizando ciertas actividades. Esto va tanto para los buenos como para los malos. En muchos casos es necesario determinar quién configuró mal algo en lugar de quién robó algo. Las pistas de auditoría basadas en códigos de acceso e identificación establecen la responsabilidad individual. Entre las preguntas que se debe abordar al revisar los registros de auditoría se incluyen las siguientes:

- ¿Los usuarios tienen acceso a la 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 autoauditorías o realizadas por un tercero. Las autoauditorías siempre introducen el peligro de la subjetividad en el proceso. Los registros se pueden generar en una amplia variedad de dispositivos, incluidos sistemas de detección de intrusos (IDS), servidores, enrutadores y conmutadores. De hecho, un IDS basado en host hace uso de los registros del sistema operativo de la máquina host.

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

- ¿La pista de auditoría proporciona un seguimiento de las acciones del usuario?
- ¿Está estrictamente controlado el acceso a los registros en línea?
- ¿Existe separación de funciones entre el personal de seguridad que administra la función de control de acceso y el que administra 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 protegidos para evitar la modificación, 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 una revisión formal de los registros de auditoría, se trata de una forma de control *administrativo detectivesco.* La revisión de los datos de auditoría debe ser una función independiente de la administración diaria del sistema.

Tipos de registro

PuntoClave12

El registro es el proceso de registrar información de eventos en un archivo de registro o base de datos. Captura eventos del sistema, cambios, mensajes y otra información que muestra las actividades que se producen en un sistema o dispositivo. Los diferentes tipos de registros que usan los profesionales de la seguridad incluyen registros de seguridad, registros de sistemas, registros de aplicación, 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 tiene acceso, modifica o elimina un archivo o carpeta. Aunque la mayoría de los sistemas registrarán cuando se accede a los archivos de claves, 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 realizadas por un usuario malintencionado.

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

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

Los registros de proxy registran detalles sobre el tráfico de Internet que pasa a través del servidor proxy, incluidos los sitios visitados por los usuarios, cuánto tiempo se pasa en esos sitios y si se está intentando acceder a sitios prohibidos.

Los registros de cambios notifican los cambios realizados en un dispositivo o aplicación específicos 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 grupos 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 de derechos y permisos para todos los usuarios. Las auditorías de grupos 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 producen acciones o accesos no autorizados, mientras que los sistemas de prevención de intrusiones (IPS) supervisan el mismo tipo de actividad, pero en realidad funcionan para evitar que las acciones se vigilen correctamente. Los dispositivos IDS e IPS se pueden utilizar durante las investigaciones para proporcionar la información con respecto a los patrones de tráfico que ocurren momentos antes de que un ataque tenga éxito. Los profesionales de la seguridad deben ajustar constantemente los dispositivos IDS e IPS para asegurarse de que se detecta o previene 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 la red".

Administración de eventos e información de seguridad (SIEM)

SIEM puede recopilar información de registros y sistemas para cumplir con los requisitos reglamentarios, proporcionar responsabilidad interna, proporcionar administración de riesgos y realizar monitoreos y tendencias. SIEM almacena información sin procesar de varios sistemas y dispositivos y agrega esa información en una sola base de datos. Los profesionales de la seguridad deben trabajar juntos para garantizar que se supervisen las acciones apropiadas y para garantizar que se produzcan los exámenes correctos de los registros. Debido a que los sistemas SIEM son repositorios centralizados de información de seguridad, las organizaciones deben tener especial cuidado de proporcionar la seguridad adecuada para estos sistemas para garantizar que los atacantes no puedan acceder o alterar 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 monitoreo debe ser parte de un programa de monitoreo continuo de la organización. El programa de monitoreo continuo debe estar diseñado para satisfacer las necesidades de la organización e implementado correctamente para garantizar que la infraestructura crítica de la organización esté vigilada. Es posible que las organizaciones deseen buscar soluciones de supervisión continua como servicio (CMaaS) implementadas por proveedores de servicios en la nube.

Supervisión de salida

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 supervisión de salida se lleva a cabo mediante firewalls que supervisan y controlan el tráfico saliente.

La fuga de datos se produce cuando los datos confidenciales se divulgan a personal no autorizado, ya sea intencionalmente o inadvertidamente. El software de prevención de pérdida de datos (DLP) intenta evitar la fuga de datos. Lo hace manteniendo el conocimiento 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 por correo electrónico. El software DLP usa filtros de entrada y salida para identificar los datos confidenciales que salen de la organización y pueden evitar dicha fuga.

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

- No se puede enviar por correo electrónico a nadie que no sean miembros del grupo de ventas.
- 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, DLP de red analiza el tráfico de red.
- **DLP de punto de conexión:** DLP de extremo se ejecuta en estaciones de trabajo o servidores de usuario final de la organización.

Puede utilizar métodos precisos e imprecisos para determinar lo que es sensible:

- **Métodos precisos:** Estos métodos implican el registro de contenido y desencadenan casi cero incidentes de 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 radica en el nivel de precisión con el que puede localizar y evitar la fuga de datos confidenciales.

Nota

La esteganografía y las marcas de agua a veces son parte del monitoreo de salida. Ambas herramientas criptográficas se discuten en el Capítulo 3,"Arquitectura e Ingeniería de Seguridad".

Lab# DLP en M365

7.4 Aprovisionamiento 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 los activos son robados o implementados incorrectamente es imposible si no existe un sistema de inventario o recuento de artículos o si el inventario no se mantiene actualizado. Todos los equipos deben ser inventariados, 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 del firmware, la versión del sistema operativo, el personal responsable, etc. La organización debe mantener esta información tanto electrónicamente como en forma impresa. El mantenimiento de este inventario ayudará a determinar cuándo deben desplegarse los nuevos bienes o cuándo deben desmantelarse los bienes actualmente desplegados.

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 pueden ser robados fácilmente, como computadoras portátiles, tabletas y teléfonos inteligentes, deben ser bloqueados. Si eso no es práctico, considere la posibilidad de bloquear estos tipos de dispositivos a objetos estacionarios (por ejemplo, el uso de bloqueos de cables con computadoras portátiles).

Cuando la tecnología está disponible, el seguimiento de dispositivos pequeños puede ayudar a mitigar la pérdida de 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 la torre celular 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, indicándolo que borre los datos contenidos en el dispositivo. Del mismo modo, estos dispositivos normalmente también vienen con la capacidad de ser bloqueados de forma remota cuando se extravía.

Un 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. Permitir la copia de datos a estos tipos de unidades, siempre y cuando los datos se cifran también es posible. Si estas funciones las proporciona el sistema operativo de red, debe implementarlas.

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

El cifrado de datos confidenciales almacenados en dispositivos puede ayudar a evitar la exposición de datos en caso de robo o en caso de acceso inadecuado 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 desplegarse y desmantelarse en función de las necesidades de la organización. Por ejemplo, supongamos que una organización implementa un punto de acceso inalámbrico (WAP) para que lo use un auditor de terceros. El aprovisionamiento apropiado del recurso debe asegurarse de que el WAP esté dado de baja una vez que el auditor de tercera parte necesita no más el acceso a la red. Sin la Administración apropiada del inventario y de la configuración, el WAP puede seguir desplegado y se puede utilizar en algún momento para realizar un ataque de red inalámbrica.

Activos virtuales

Los activos virtuales incluyen redes definidas por software, redes de área de almacenamiento virtual (VSANs), sistemas operativos invitados implementados en máquinas virtuales (VM) y enrutadores virtuales. Al igual que con los activos físicos, la implementación y retirada de activos virtuales debe 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 Windows Server 2016 debe conservarse solo hasta que ya no sea necesaria. Mientras 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 virtual 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 usa 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 garantizar que solo se implementen 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). Debe mantenerse el número adecuado de licencias para todas las aplicaciones comerciales. Una organización debe revisar periódicamente sus necesidades de licencias. Para las implementaciones en la nube de servicios de software, la administración de la configuración debe usarse para garantizar que solo el personal que tiene necesidades válidas para el software tenga acceso a él.

Administración de la configuración

Aunque en realidad es un subconjunto de la administración de cambios, la administración de la configuración se centra específicamente en poner orden en el 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 más importancia aquí, teniendo en cuenta el impacto que los cambios en conflicto pueden tener (y en algunos inmediatamente) en una red.

PuntoClave13

Las siguientes son las funciones de administración de la configuración:

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

Nota

En el contexto de la gestión de la configuración, una biblioteca de *software* es un área controlada accesible sólo 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 está sujeta a un procedimiento de control de configuración independiente. Cuando una operación se divide en CIs individuales, el proceso se denomina *identificación de configuración.*

Ejemplos de estos tipos 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 ser documentados, y todos los diagramas de red, tanto lógicos como físicos, *deben* actualizarse constante y consistentemente para reflejar con precisión el estado de cada configuración *ahora* y no como era hace dos años. La comprobación de que se siguen 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 introducidos 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

7.5 Conceptos de operaciones de seguridad

A lo largo de este libro, ha visto referencias a directivas y principios que pueden guiar todas las operaciones de seguridad. En esta sección, revisamos algunos conceptos más completamente

que ya se han tocado e introducimos algunos nuevos problemas relacionados con el mantenimiento de las operaciones de seguridad.

Necesidad de saber/privilegios mínimos

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 recursos, eso significa que el nivel predeterminado de acceso debe ser *sin acceso.* Proporcione a los usuarios acceso solo a los recursos necesarios para realizar su trabajo, y ese 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 conocerlo un usuario. Para garantizar que los privilegios mínimos requieren que se identifique el trabajo del usuario y que se conceda a cada usuario la autorización más baja necesaria para sus tareas. Otro ejemplo es la implementación de vistas en una base de datos. Necesidad de saber requiere que el operador tenga el conocimiento mínimo 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. Las cuentas de usuario se crean 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 con mayor frecuencia los roles.

Los profesionales de la seguridad deben entender 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 dicha cuenta 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 mantener estas cuentas, la mayoría de los proveedores sugieren que cambie el nombre de la cuenta y le asigne una contraseña compleja. Las cuentas raíz o de administrador solo se deben usar al realizar tareas administrativas, y el uso de estas cuentas siempre debe auditarse.
- **Cuentas de servicio:** Estas cuentas se utilizan para ejecutar aplicaciones y servicios 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 utilizan. Asegúrese de cambiar las contraseñas de estas cuentas de forma regular. El uso de estas cuentas siempre debe ser auditado.

- **Cuentas de administrador normales:** Estas cuentas de administrador se crean y se asignan solo a una sola persona. Cualquier usuario que tenga una cuenta administrativa también debe tener una cuenta de usuario normal o estándar para usarla en las operaciones normales del día a día. Las cuentas administrativas solo se deben usar al realizar tareas de nivel administrativo, y el uso de estas cuentas siempre debe auditarse.
- **Cuentas de usuario potencia:** Estas cuentas tienen más privilegios y permisos que las cuentas de usuario normales. Estas cuentas deben revisarse periódicamente 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 usan mientras realizan sus tareas de trabajo diarias normales. Estas cuentas deben seguir estrictamente el principio de privilegios mínimos.

Separación de deberes y responsabilidades

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

Administración de cuentas con privilegios

Los profesionales de la seguridad deben asegurarse de que las organizaciones establezcan los procedimientos adecuados de administración del ciclo de vida de cuentas, grupos y roles para asegurarse de que se crean, administran y quitan correctamente. El ciclo de vida del aprovisionamiento se trata con más detalle en el capítulo 5,"Administración de identidad y acceso (IAM)".

Inevitablemente, algunos usuarios, especialmente los supervisores o los del departamento de soporte técnico de TI, requerirán derechos y privilegios especiales que otros usuarios no poseen. Por ejemplo, podría ser necesario que un conjunto de usuarios que trabajan en el departamento de soporte técnico necesiten poder restablecer las contraseñas o quizás realizar cambios en las cuentas de usuario. Este tipo de derechos conllevan la responsabilidad de ejercerlos 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 trabajo y vacaciones obligatorias

Desde una perspectiva de seguridad, la rotación de trabajo se refiere a la capacitación de múltiples 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 se note actividades inusuales por parte de cualquier persona. Esto se utiliza a menudo en conjunción con *las vacaciones obligatorias,*en las que todos los usuarios están obligados a tomar tiempo libre, lo que permite a otro para llenar su posición mientras se ha ido, lo que mejora la oportunidad de descubrir una actividad inusual. Más allá de los aspectos de seguridad de la rotación de puestos de trabajo, los beneficios adicionales incluyen

- Backup 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 controles administrativos.

Control de dos personas

Un control de dos personas, también conocido como una regla de dos personas, se produce 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 encima de una cierta cantidad de dólares o que dos personas estén presentes para realizar una determinada actividad, como abrir una caja fuerte.

Procedimientos de información confidencial

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 un mínimo de vergüenza para la empresa 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 los procedimientos y políticas de control de acceso, es necesario responder a las siguientes preguntas:

- ¿Hay datos disponibles para el usuario que no son necesarios para su trabajo?
- ¿Demasiados usuarios tienen acceso a datos confidenciales?

Retención de registros

El control de acceso adecuado no es posible sin la auditoría. Esto nos permite realizar un seguimiento de las actividades y descubrir problemas antes de que se realicen por completo. Debido a que esto a veces puede conducir a una montaña de datos para analizar, solo supervise las actividades más sensibles y conserve y revise todos los registros. Además, en muchos casos las empresas están obligadas por ley o reglamento a mantener registros de ciertos datos.

La mayoría de los sistemas de auditoría permiten la configuración de opciones de retención de datos. En algunos casos, la operación predeterminada es empezar a escribir sobre los registros más antiguos del registro cuando el tamaño máximo del registro está lleno. La limpieza y el almacenamiento regulares del registro pueden evitar que esto suceda y evitar la pérdida de eventos importantes. En casos de datos extremadamente confidenciales, incluso es aconsejable que un servidor cierre el acceso 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 deactivos".

Acuerdos de nivel de servicio

Los acuerdos de nivel de servicio (SLA) son acuerdos sobre la capacidad del sistema de soporte para responder a los problemas dentro de un plazo determinado 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 que se abordan los diversos problemas, se introduce cierta previsibilidad en la respuesta a los problemas, lo 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 las 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 escalamiento y el costo. Debe incluir una cláusula relativa al pago a los clientes resultante de un incumplimiento del SLA. Si bien los SLA pueden ser transferibles, no lo son 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, se deben revisar las métricas, las herramientas de medición y los procesos para ver si han mejorado.

7.6 Protección de recursos

Los recursos empresariales incluyen tanto activos que podemos ver y tocar (tangibles), como computadoras e impresoras, como activos que no podemos ver y tocar (intangibles), como secretos comerciales y procesos. Aunque normalmente pensamos en la protección de 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 el mantenimiento de la disponibilidad de esos recursos. En esta sección, trataremos ambos aspectos de la protección de los 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 el terreno circundante. La seguridad física se trata más adelante en este capítulo, pero vale la pena enfatizar que las pruebas de vulnerabilidad (discutidas más a fondo en el Capítulo 6)deben incluir los controles de seguridad de la propia instalación. Algunos ejemplos de pruebas de vulnerabilidad en relación con 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 zonas sensibles, como las salas de servidores y los armarios de cableado?
- ¿Funciona el sistema de extinción de incendios?
- ¿Se trituran los documentos sensibles en lugar de tirarse al contenedor de basura?

Más allá de los problemas de acceso, los principales sistemas que se necesitan para garantizar que las operaciones no se interrumpan incluyen la detección / supresión de incendios, HVAC

(incluidos los controles de temperatura y humedad), los sistemas de agua y alcantarillado, la energía de energía / respaldo, los equipos de comunicaciones y la detección de intrusiones.

Hardware

Otro de los activos más tangibles que hay que proteger es todo el hardware que hace funcionar la red. Esto incluye no solo los equipos e impresoras con los que los usuarios entran en contacto directo, sino también los dispositivos de infraestructura que nunca ven, como enrutadores, conmutadores y dispositivos de firewall. Mantener el acceso a estos dispositivos críticos desde el punto de vista de la disponibilidad se trata más adelante en las secciones"Redundancia y tolerancia a fallos"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 funciones de administración, así como para proteger los datos y los comandos que pasan a través de la red a estos dispositivos. Algunas pautas 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 texto no cifrado), utilice una herramienta de línea de comandos cifrada como Secure Shell (SSH).
- Administre los 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 han desarrollado internamente y que son críticos para el funcionamiento de la organización. Las prácticas seguras de codificación y desarrollo pueden ayudar a prevenir debilidades en estos sistemas. También hay que prestar atención a la prevención del robo de estos activos.

Además, la vigilancia estrecha del uso de aplicaciones y sistemas comerciales en la empresa puede evitar el incumplimiento involuntario de los acuerdos de licencia. Uno de los beneficios de solo dar a los usuarios las aplicaciones que necesitan para hacer su trabajo es que limita el número de usuarios que tienen una aplicación, lo que ayuda a evitar el agotamiento de las licencias de software.

Nota

La seguridad del desarrollo de software se describe en detalle en el capítulo 8,"Seguridad de desarrollo desoftware".

Activos de información

Los activos de información son el último tipo de activo que necesita ser discutido, pero de ninguna manera son los menos importantes. El propósito *principal* de la seguridad de las operaciones es proteger 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 puede ser difícil de determinar, aunque puede estar claro para todos los involucrados que el activo es crítico. Por ejemplo, la fórmula secreta de Coca-Cola ha estado estrechamente vigilada 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 eliminación, 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 errores

Una forma de proporcionar acceso ininterrumpido a los activos de información es a través de la redundancia y la tolerancia a errores. La redundancia hace referencia a proporcionar varias instancias de un componente físico o lógico de forma 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 la redundancia, pero se refiere a cualquier proceso que permita a un sistema continuar haciendo que los activos de información estén disponibles en caso de una falla.

En algunos casos, la redundancia se aplica en la capa física, como la redundancia de red proporcionada por una red troncal 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 por ejemplo cuando un router sabe las trayectorias múltiples a un destino en caso de que uno falle.

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 se refiere a sistemas como la matriz redundante de discos independientes (RAID) en la que los datos se escriben en varios discos de tal manera que un disco puede fallar y los datos pueden estar disponibles rápidamente desde los discos restantes de la matriz sin tener que recurrir a una cinta de copia de seguridad. Familiarícese con varios tipos de 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 Backup y Recuperación

Aunque a lo largo de este capítulo se encuentra una amplia cobertura de los sistemas de copia de seguridad y recuperación, es importante destacar aquí el papel de las operaciones en la realización de esas actividades. Una vez diseñada la programación de copia de seguridad, habrá tareas diarias asociadas con 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 puedan 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.

Administración de identidad y acceso

Desde una perspectiva de operaciones, es importante tener en cuenta que la administración de estas cosas es un proceso continuo que puede requerir la creación de cuentas, la eliminación de cuentas, la creación y rellenación de grupos y la administración de los permisos asociados con todos estos conceptos. Es esencial asegurarse de que los derechos para realizar estas acciones están estrictamente controlados y de que se establece un proceso formal para quitar permisos cuando ya no son necesarios y deshabilitar las cuentas que ya no son necesarias.

Otra área en la que centrarse es el control del uso de cuentas con privilegios o cuentas que tienen derechos y permisos que superan los de una cuenta de usuario normal. Aunque esto obviamente se aplica a las cuentas integradas de administrador, raíz o supervisor (que en algunos sistemas operativos se denominan cuentas raíz) que tienen permisos amplios, también se aplica a cualquier cuenta que confiera privilegios especiales al usuario.

Además, mantenga el mismo control estricto sobre los numerosos grupos integrados que existen en Windows para conceder derechos especiales a los miembros del grupo. Al utilizar estos grupos, anote los privilegios de los grupos predeterminados que no sean necesarios para sus fines. 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 gestión de identidades y accesos en el capítulo 5.

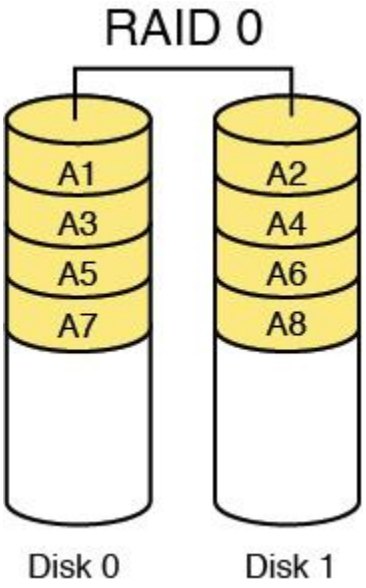
Administración de medios

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) se refiere a un sistema mediante el cual se utilizan varias unidades de disco duro para proporcionar un aumento del rendimiento o tolerancia a errores para los datos. Cuando hablamos de tolerancia a fallos en RAID, nos referimos a mantener el acceso a los datos incluso en un fallo de la unidad sin restaurar los datos de los medios de copia de seguridad. Los siguientes son los tipos de RAID con los que debe estar familiarizado.

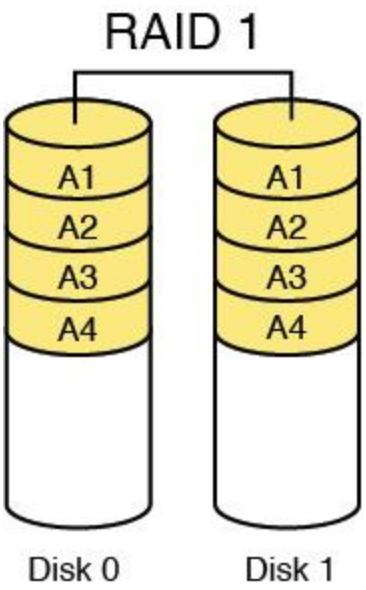
*RAID 0,*también denominado sección de disco, escribe los datos en varias unidades. Aunque mejora el rendimiento, no proporciona tolerancia a errores. La figura 7-3 representa RAID 0.



Hay dos pilas de discos circulares en los que el de la izquierda, etiquetado disco 0 tiene discos de arriba a abajo que lee A1, A2, A3, A4 y la parte restante se deja vacía. El de la derecha etiquetado disco 1 tiene discos de arriba a abajo que lee A2, A4, A6, A8 y la parte restante se deja vacía. Las dos pilas están unidas por un conector etiquetado, RAID 0.

Figura 7-3 RAID 0

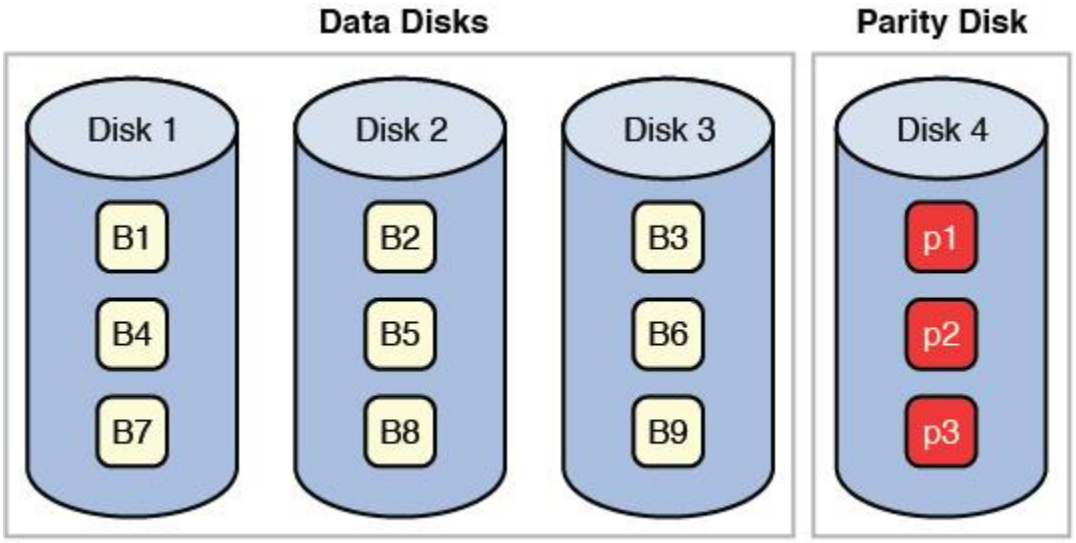
*RAID 1,*también llamado duplicación de disco, utiliza dos discos y escribe una copia de los datos en ambos discos, proporcionando tolerancia a errores en el caso de un error de una sola unidad. La Figura 7-4 representa RAID 1.



Hay dos pilas de discos circulares en los que el de la izquierda, etiquetado disco 0 tiene discos de arriba a abajo que lee A1, A2, A3, A4 y la parte restante se deja vacía. El de la derecha etiquetado disco 1 tiene discos de arriba a abajo que lee A1, A2, A3, A4 y la parte restante se deja vacía. Las dos pilas están unidas por un conector etiquetado, 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 la creación de bandas, y luego que la *información de paridad* se escriba en una sola unidad dedicada. La información de paridad se utiliza para regenerar los datos en el caso de un fallo de una sola unidad. La caída es que la unidad de paridad es un único punto de falla si va mal. La Figura 7-5 representa RAID 3.

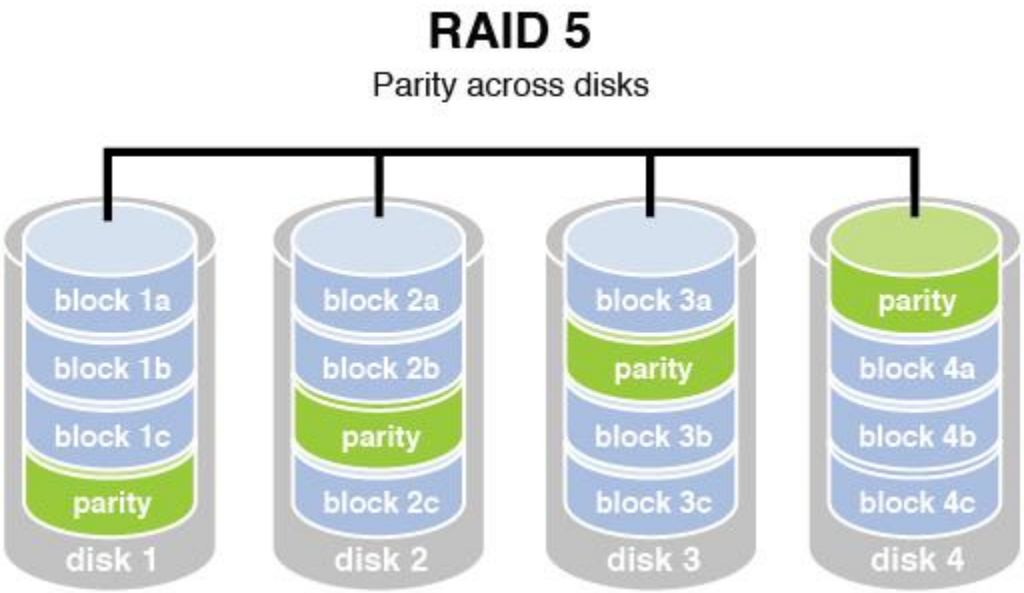


RAID 3 – Bytes Striped (and Dedicated Parity Disk)

Dos bloques, Discos de Datos- compuestos por cilindros, Disco 1, Disco 2 y Disco 3; y disco de paridad- que comprende de un cilindro, disco 4 se muestran uno al lado del otro. Cilindros disco 1, disco 2 y disco 3 del bloque de discos de datos constan de bloques que leen, B1, B4 y B7; B2, B5 y B8; y B3, B6 y B9, respectivamente. El disco 4 cilindro se compone de bloques que leen, p1, p2 y p3. El texto debajo de los bloques leídos, RAID 3 - Bytes seccionados (y disco de paridad dedicado).

Figura 7-5 RAID 3

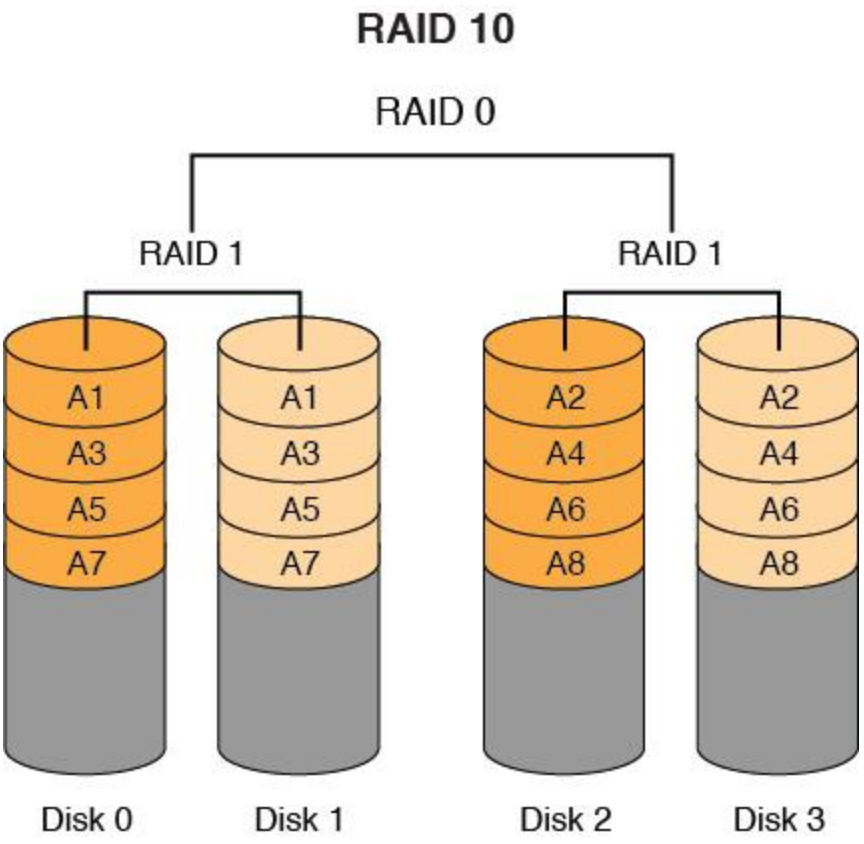
*RAID 5,*que requiere al menos tres unidades, también requiere que los datos se escriban en todas las unidades, como la creación de bandas, y luego que la información de paridad también se escriba en todas las unidades. La información de paridad se utiliza de la misma manera que en RAID 3, pero no se almacena en una sola unidad, por lo que no hay un único punto de falla para los datos de paridad. Con el nivel RAID de hardware 5, las unidades de repuesto que reemplazan las unidades fallidas 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.



Hay cuatro pilas de discos: disco 1, disco 2, disco 3 y disco 4, de izquierda a derecha, interconectados entre sí. La composición de los cuatro discos es la siguiente (de arriba a abajo): Disco 1- bloque 1a, bloque 1b, bloque 1c y paridad; Disco 2: bloque 2a, bloque 2b, paridad y bloque 2c; disco 3- bloque 3a, paridad, bloque 3b, y bloque 3c; y disco 4- paridad, bloque 4a, bloque 4b y bloque 4c.

Figura 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 duplicando dos unidades juntas. A continuación, se crea un conjunto de bandas RAID 0 en cada par reflejado. La Figura 7-7 representa RAID 10.



Hay dos conjuntos de cuatro pilas de discos circulares, colocados uno al lado del otro. Cada conjunto está etiquetado como 'Raid 1'. Raid 1 a la izquierda consta de dos discos disco 0 y disco 1 que tiene discos de arriba a abajo etiquetados A1, A3, A5, A7 y la parte restante se deja vacía. Raid 1 a la derecha consta de dos discos disco 2 y disco 3 que tiene discos de arriba a abajo etiquetados A2, A4, A6, A8 y la parte restante se deja vacía. Los dos Raid 1 a la izquierda y a la derecha están unidos por un conector, Raid 0.

Figura 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 de RAID que son más rápidos cuando se implementan con hardware. Sin embargo, las bandas o duplicación simples (RAID 0 y 1) tienden a funcionar bien en el software porque no utilizan las unidades de paridad a nivel de hardware. En la Tabla 7-1 se resumen los tipos de RAID.

PuntoClave14

Tabla 7-1 Niveles raid

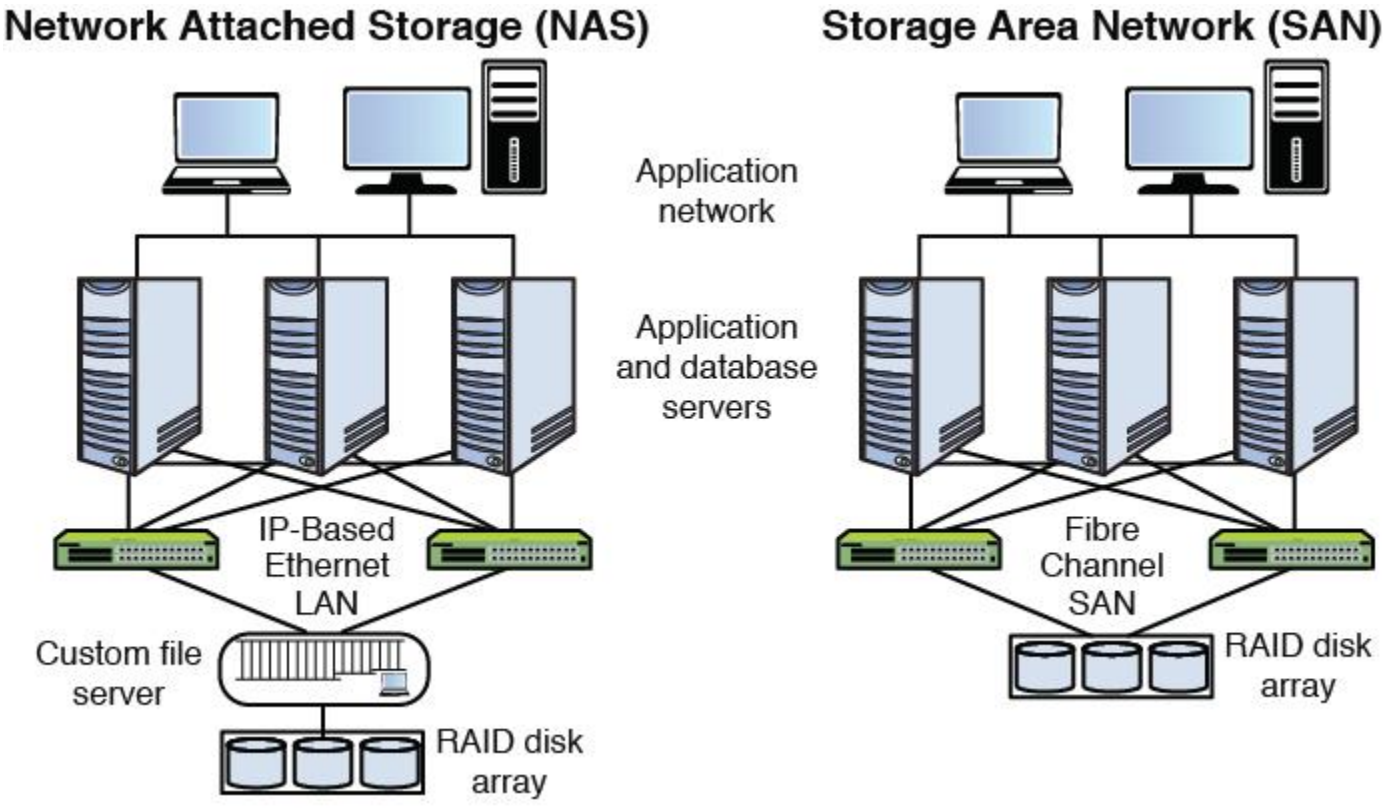
Nivel RAID	Número mínimo de unidades	Descripción	Fortalezas	Debilidades
RAID 0	2	Creación de bandas de datos sin redundancia	El más alto rendimiento	No hay protección de datos; una unidad falla, se pierden todos los datos
RAID 1	2	Espejado de disco	Muy alto rendimiento; protección de datos muy alta; penalización muy mínima en el rendimiento de escritura	Alto costo de redundancia de gastos generales; dado que todos los datos están duplicados, se requiere el doble de capacidad de almacenamiento
RAID 3	3	Bandas de datos a nivel de bytes con unidad de paridad dedicada	Excelente rendimiento para solicitudes de datos grandes y secuenciales	No es adecuado para aplicaciones de red orientadas a transacciones; una sola unidad de paridad no admite varias solicitudes simultáneas de lectura y escritura
RAID 5	3	Creación de bandas 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; admite 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	Espejado de disco con bandas	La misma tolerancia a errores que RAID 1; la misma sobrecarga que con la creación de reflejos; proporciona altas tasas de E/S; puede soportar múltiples fallas simultáneas de unidades	Muy caro; todas las unidades deben moverse en paralelo para realizar un seguimiento adecuado, 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 de almacenamiento. Esta arquitectura de información de almacenamiento aborda la recopilación de datos, la administración de datos y el uso de datos.

OA2

El almacenamiento conectado en 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 que esté interconectada a la LAN a través de una WAN) puede usar protocolos como NFS, CIFS o HTTP para conectarse a un NAS y compartir archivos. En una SAN, solo los dispositivos que pueden usar la red SCSI de canal de fibra 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.



El almacenamiento conectado a la red consiste en una matriz de discos RAID conectada a un servidor de archivos personalizado que, a su vez, está conectado a conmutadores de LAN Ethernet basada en IP. Estos conmutadores están conectados a servidores de aplicaciones y bases de datos, que también están conectados entre sí y a la red de aplicaciones. La red de área de almacenamiento consiste en una matriz de discos RAID que está conectada a switches de un canal de fibra S A N. Estos conmutadores están conectados a servidores de aplicaciones y bases de datos, que también están conectados entre sí y a la red de aplicaciones.

Figura 7-8 NAS y SAN

HSM

Un sistema de administración jerárquica de almacenamiento de información (HSM) es un tipo de sistema de administración de copias de seguridad que proporciona una copia de seguridad en línea continua mediante el uso de "jukeboxes" ópticos o de cinta. Funciona moviendo automáticamente los datos entre medios de almacenamiento de alto costo y de 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 a corto plazo para datos cambiantes, pero que requieren un acceso a archivos más rápido que la cinta.

Nota

No confunda el acrónimo HSM. HSM también puede hacer referencia al módulo de seguridad de hardware, que es un dispositivo que administra y protege las claves digitales para una autenticación segura.

Historia de los medios de comunicación

Mantenga con precisión los registros de la biblioteca de medios para realizar un seguimiento del historial de los medios. Esto es importante porque todos los tipos de medios tienen un número máximo de veces que se pueden utilizar de forma segura. Un bibliotecario de medios debe mantener 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 unidades USB). Con respecto a los medios de copia de seguridad, utilice las siguientes directrices:

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

Etiquetado y almacenamiento de medios

Etiquete claramente todas las formas de medios de almacenamiento (cintas, medios ópticos, 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.
- Asegurar 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.

The environment where the media will be stored is also important. For example, damage starts occurring to magnetic media above 100 degrees. The *Forest Green Book* is a Rainbow Series book that defines the secure handling of sensitive or classified automated information system memory and secondary storage media, such as degaussers, magnetic tapes, hard disks, and cards. The Rainbow Series is discussed in more detail in Chapter 3.

Desinfección y eliminación de medios

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 los medios de almacenamiento magnéticos, como un casete de cinta magnética, es a través de la desmagnetación, que expone los medios a un campo magnético potente y alterno. Elimina cualquier dato escrito previamente, dejando el medio en un estado aleatorio magnético (en blanco). Algunos otros términos y conceptos de eliminación con los que debe estar familiarizado son:

- **Purga de datos:** Usar un método como la desgaussificación para que los datos antiguos no estén disponibles incluso con análisis forenses. La purga hace que la información sea irrecuperable contra ataques de laboratorio (forenses).
- **Compensación de datos:** Hace que la información sea 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 de comunicación hayan sido borrados.

Administración 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 mantengan la disponibilidad de los recursos a pesar de los errores de hardware o software en el entorno. Los siguientes principios y conceptos están disponibles para ayudar a mantener el acceso a los recursos:

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

- **Tecnologías tolerantes a fallos:** Llevando la idea de redundancia al siguiente nivel son tecnologías que se basan en múltiples sistemas informáticos que trabajan juntos para proporcionar un acceso ininterrumpido, incluso en el caso de una falla de uno de los sistemas. La agrupación en clústeres de servidores y la computación en red son excelentes 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 plazo determinado 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 que se abordan los diversos problemas, se introduce cierta previsibilidad en la respuesta a los problemas, lo 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 adquieren. Los proveedores suelen publicar valores para el tiempo medio entre errores (MTBF) de un producto, que describe la frecuencia con la que un componente falla en promedio. Otra métrica valiosa que normalmente se proporciona es el tiempo medio de reparación (MTTR), que describe la cantidad promedio de tiempo que se tardará en reparar el dispositivo y volver a estar 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 podría interrumpir el acceso a los recursos si se produce un error. Cada SPOF debe mitigarse de alguna manera.

7.7 Gestión de incidentes

La respuesta a incidentes y la administración son vitales para cada organización para garantizar que se detecten, contenga e investiguen los incidentes de seguridad. La respuesta a incidentes es el comienzo de cualquier investigación. Una vez descubierto un incidente, el personal de respuesta a incidentes realiza tareas específicas. Durante toda la respuesta al incidente, el equipo de respuesta al incidente debe asegurarse de que siguen los procedimientos adecuados para garantizar que se conserven las pruebas. La gestión de incidentes garantiza que el equipo de respuesta a incidentes gestione el incidente y devuelva el servicio a la normalidad lo antes posible después de un incidente.

Como parte de la respuesta a incidentes, los profesionales de la seguridad deben comprender la diferencia entre eventos e incidentes (consulte la sección siguiente). El equipo de respuesta a incidentes debe contar con los procedimientos de respuesta a incidentes adecuados para garantizar que se maneje el incidente, pero los procedimientos no deben obstaculizar las investigaciones forenses que puedan ser necesarias para garantizar que las partes sean responsables de cualquier acción ilegal. Los profesionales de la seguridad deben comprender las reglas de compromiso 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 un impacto negativo en 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 se producen muchos intentos de inicio de sesión no válidos durante un período de unas pocas horas, la organización podría estar 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 todos 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 tener en cuenta los conocimientos técnicos de cada individuo. Los miembros del equipo deben comprender la directiva 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 competentes.

El equipo de respuesta a incidentes debe tener acceso al plan de respuesta a incidentes. Este plan debe incluir la lista de autoridades con las que ponerse en contacto, las funciones y responsabilidades del equipo, una lista de contactos interna, procedimientos para obtener y preservar pruebas y una lista de expertos en investigación con los que se puede contactar 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 omite ningún paso. Una vez iniciado el proceso de respuesta a incidentes, 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 con la alta dirección y las autoridades correspondientes.

Reglas de contratación, autorización y ámbito

Una organización debe documentar las reglas de compromiso, autorización y ámbito para el equipo de respuesta a incidentes. Las reglas de compromiso 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 realizar una investigación y el alcance permitido de cualquier investigación que deban emprender.

Las reglas de compromiso actúan como una guía para que el equipo de respuesta a incidentes se asegure de que no cruzan la línea de la tentación a la trampa. La tentación ocurre cuando se proporciona la oportunidad de acciones ilegales (atraer) pero el atacante toma su propia decisión de realizar la acción, y la trampa significa alentar a alguien a cometer un delito que el individuo podría no haber tenido intención de cometer. La tentación es legal, pero plantea argumentos éticos y podría no ser admisible en los tribunales. Por el contrario, el atrapamiento es ilegal.

PuntoClave15

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 busque, 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. Detectar el incidente.
2. Responder al incidente.
3. Mitigar los efectos del incidente.
4. Reporte el incidente al personal apropiado.
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 como lecciones aprendidas.

La investigación real del incidente se produce durante los pasos de respuesta, mitigación, notificación y recuperación. Después de los procesos de investigación forense y digital apropiados durante la investigación puede garantizar que se preserven 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

Los eventos de seguridad ocurrirán inevitablemente, 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 bien 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 primero deben realizar el triaje apropiado para los activos afectados. Esto incluye detectar inicialmente el incidente y determinar la gravedad del incidente. En algunos casos, durante la fase de triaje, los profesionales de seguridad pueden determinar que se ha producido un falso positivo, lo que significa que un ataque realmente no se produjo, aunque una alerta indicara que sí se produjo. Si se confirma un ataque, la respuesta al incidente avanzará en acciones de investigación.

Todos los controles 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 mouse que falta en la sala de servidores. Establezca respuestas estándar y tiempos de respuesta con anticipación.

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

Después de que un ataque es 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 adecuadas con respecto al incidente. Una vez determinada la causa raíz, los

profesionales de seguridad deben seguir las directivas de control de incidentes que la organización tiene en vigor.

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 alcance de activos. Las opciones de mitigación varían en función del tipo de ataque que se haya producido. Los profesionales de la seguridad deben desarrollar procedimientos de antemano que detallen cómo mitigar correctamente los ataques que se producen contra los activos de la organización. La preparación anticipada de estos procedimientos de mitigación 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. Es fundamental prestar atención a los detalles en esta etapa temprana mientras la información sensible al tiempo todavía está disponible.

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 bienes 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 la restauración del servidor a partir de una copia de seguridad reciente. El objetivo principal de este paso es hacer que todos los recursos estén disponibles de nuevo. Retrasar la puesta en funcionamiento de cualquier activo hasta que al menos esté protegido del incidente que se produjo. Pruebe a fondo los activos para detectar vulnerabilidades y debilidades antes de reintroducirlos en la producción.

Remediar

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

Lecciones aprendidas y revisión

Finalmente, revise cada incidente para descubrir qué se podría aprender de él. Es posible que se 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 y el análisis completos son el objetivo de este paso.

7.8 Detective and Preventive Measures

PuntoClave16

Como probablemente ya haya reunido, una amplia variedad de amenazas de seguridad se enfrenta a los encargados de proteger los activos de una organización. Afortunadamente, una amplia variedad de herramientas está disponible para usar para llevar a cabo esta tarea. En esta sección se tratan algunas amenazas comunes y enfoques de mitigación.

IDS/IPS

La instalación, configuración y supervisión de cualquier sistema de detección de intrusiones y prevención de intrusiones (IDS/IPS) también son responsabilidades permanentes 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 ataque. Los motores de análisis que utilizan también a veces tienen actualizaciones que deben aplicarse.

Además, los archivos de registro de los sistemas que están configurados para registrar ciertos eventos en lugar de realizar acciones específicas cuando se producen necesitan tener esos registros archivados y analizados de forma regular. Gastar grandes sumas de dinero en software que recopila información y luego ignorar esa información no tiene sentido.

Ids e IPS se discuten con más detalle anteriormente en este capítulo y en el capítulo 4.

La respuesta a intrusiones 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 los 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 evitar la comunicación en función de una variedad de factores. Si el personal descubre que se están produciendo ciertos tipos de tráfico no deseado, a menudo es bastante sencillo configurar un firewall para evitar ese tipo de tráfico. Los firewalls pueden proteger los límites entre redes, el tráfico dentro de una subred o un único sistema. Asegúrese de mantener los firewalls totalmente actualizados según las recomendaciones del proveedor. Los cortafuegos se analizan con más detalle en el capítulo 4.

Listas blancas/listas negras

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 como se permite. La lista negra identifica a los remitentes incorrectos. La lista gris se encuentra en algún lugar entre los dos, enumerando las entidades que no se pueden identificar como elementos de la lista blanca o negra. En el caso de la lista gris, la nueva entidad debe pasar por una serie de pruebas para determinar si estará en la lista blanca o en la lista negra.

Las listas blancas, negras y grises se utilizan comúnmente con las herramientas de filtrado de spam.

Servicios de seguridad de terceros

Es posible que los profesionales de la seguridad deban confiar en servicios de seguridad de terceros para encontrar amenazas en la empresa. Algunos servicios de seguridad comunes de terceros incluyen detección de malware/virus y honeypots/honeynets. A menudo es más fácil confiar en una solución desarrollada por un tercero que intentar desarrollar su propia solución interna. Investigue siempre 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.

Espacio aislado

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 del entorno limitado no pueden realizar cambios permanentes en el sistema y sus archivos.

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

Honeypots/Honeynets

Honeypots son sistemas que están 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 solo 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 software antivirus y antimalware son responsabilidad de la seguridad de las operaciones. Es importante implementar una solución antimalware/antivirus integral para toda la empresa.

Niveles de recorte

Los niveles de recorte establecen una línea base para los errores normales del usuario, y las infracciones que superen ese umbral se registrarán 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 el registro de actividades comienza cuando se supera un determinado nivel.

Los niveles de recorte se utilizan para

- Reducir la cantidad de datos que se evaluarán en los registros de auditoría
- Proporcionar una línea de base de errores de usuario por encima de los cuales se registrarán las infracciones

Nota

Los niveles de recorte también se tratan 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 de base para el rendimiento de determinados sistemas. Una vez establecidos estos puntos de referencia, se pueden identificar desviaciones para las normas. Esto es especialmente útil en la identificación de ciertos tipos de ataques DoS a medida que ocurren. Más allá de la ventaja de seguridad, también ayuda a identificar los sistemas que podrían necesitar actualización 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 aceptarse como una respuesta cuando se producen problemas. Aunque el enfoque suele estar en poner los sistemas en funcionamiento de nuevo, se deben identificar las causas raíz de los problemas. Evite la tentación de implementar una solución rápida (a menudo a expensas de la seguridad). Cuando el tiempo lo permite, es mejor usar un enfoque metódico para encontrar exactamente por qué ocurrió el evento, 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. Disponer de la supervisión del sistema para registrar todos los reinicios del sistema e investigar los que no hayan sido iniciados por un humano o que se hayan producido como resultado de una actualización automática.

Divulgación no autorizada

La divulgación no autorizada de información es una gran amenaza para las organizaciones. Incluye destrucción de información, interrupción del servicio, robo de información, corrupción de información y 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 incumpla la seguridad cuando se produce un bloqueo del sistema u otro error del sistema. Es posible que recuerde en el capítulo 3 que el *Libro Naranja* requiere que un sistema sea capaz de una recuperación confiable para todos los sistemas clasificados como B3 o A1.

Rutas de acceso 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.* Llevando esto un 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 validan 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

La idea principal 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 de datos y el formato 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 de salida confidencial debe requerir un recibo antes de la liberación y tener los controles de acceso adecuados aplicados independientemente de su formato.

Endurecimiento del sistema

Otro de los objetivos continuos de la seguridad de las operaciones es garantizar que todos los sistemas se han endurecido en la medida de lo posible y aún así proporcionan funcionalidad. El endurecimiento se puede lograr sobre una base física y sobre una base lógica. La seguridad física de los sistemas se trata en detalle más adelante en este capítulo. Desde una perspectiva lógica

- Quitar aplicaciones innecesarias.
- Deshabilite los servicios innecesarios.
- Bloquear puertos no adquiridos.
- Controle firmemente la conexión de dispositivos de almacenamiento externos y medios si está permitido.

Sistemas de gestión de vulnerabilidades

La importancia de realizar pruebas de vulnerabilidad y penetración se ha enfatizado a lo largo de este libro. Un sistema de gestión de vulnerabilidades es un software que centraliza y hasta cierto punto automatiza el proceso de monitorización y prueba continua de vulnerabilidades en la red. Estos sistemas pueden escanear la red en busca de vulnerabilidades, reportarlas y, en muchos casos, remediar 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 tomar el lugar de las pruebas de vulnerabilidad y penetración realizadas por profesionales capacitados.

Administración de parches y vulnerabilidades

La administración de revisiones a menudo se ve como un subconjunto de la administración de la configuración. *Los parches de software* son actualizaciones publicadas por 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 instaladas las revisiones más recientes, implemente un sistema formal para asegurarse de que todos los sistemas reciben las actualizaciones más recientes *después* de realizar pruebas exhaustivas en un entorno que no sea de producción. Es imposible para el proveedor anticipar cada posible impacto 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.

PuntoClave17

El ciclo de vida de la administración de revisiones incluye los siguientes pasos:

1. **Priorización y programación de parches:** Determine la prioridad de las revisiones y programe las revisiones para su implementación.
2. **Pruebas de parches:** Pruebe las revisiones antes de la implementación para asegurarse de que funcionan correctamente y no causan problemas de seguridad o del sistema.
3. **Instalación de parches:** Instale los parches en el entorno activo.
4. **Evaluación y auditoría de parches:** Una vez implementados los parches, asegúrese de que los parches funcionan correctamente.

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

La administración de vulnerabilidades identifica, clasifica, corrige y mitiga las vulnerabilidades en sistemas y aplicaciones. Las herramientas de administración de vulnerabilidades, también conocidas como analizadores de vulnerabilidades, deben usarse para evaluar regularmente la red, los sistemas y las aplicaciones. Se deben investigar todas las vulnerabilidades identificadas y se deben tomar las medidas de corrección o mitigación adecuadas. Nessus es un popular escáner de vulnerabilidades 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 analizadores de vulnerabilidades tengan los archivos de firma más recientes.

Procesos de gestión de cambios

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 gestionar el cambio de una 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 analizarse para asegurarse de que admite todos los objetivos y políticas. Esto incluye la línea de base y el análisis del impacto en la seguridad.
- Antes de la aprobación oficial, deberían revisarse todos los costos y efectos de los métodos de aplicación. Con los datos recopilados, los cambios deben ser aprobados o denegados.
- Una vez aprobados, se deben desarrollar los pasos de cambio.
- Durante la implementación, deben producirse pruebas incrementales y deben basarse en una estrategia de reserva predeterminada si es necesario. El control de versiones se debe usar para realizar un seguimiento y controlar eficazmente los cambios en una colección de entidades.
- La documentación completa debe ser producida y presentada con un informe formal a la gerencia.

Una de las ventajas clave 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.

7.9 Estrategias de recuperación

La identificación de los controles preventivos es el tercer paso de los pasos de continuidad del negocio como se describe en NIST SP 800-34 R1. Si se identifican controles preventivos en el análisis de impacto en el negocio (BIA), los desastres o eventos disruptivos podrían mitigarse o eliminarse. 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, las instalaciones y la energía redundantes; tecnologías de tolerancia a fallos; seguros; 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 una operación exitosa. *Las* estrategias de recuperación de nivel superior identifican el orden en que se restauran los procesos y las funciones. *Las* estrategias de recuperación a nivel de sistema definen cómo se va a restaurar un sistema determinado. Tenga en cuenta que las personas que mejor entienden el sistema deben definir estrategias de recuperación del sistema. Aunque el comité de planeación de la continuidad del negocio (BCP) probablemente pueda desarrollar las listas de recuperación priorizado y las estrategias de recuperación de alto nivel, los administradores de sistemas y otro personal de TI deben participar en el desarrollo de estrategias de recuperación para los 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 debería requerir la formación de 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 con antelación e incorporarse en el 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 la recuperación en casos de desastre, el comité del plan de recuperación debe ponerse en contacto con los proveedores críticos con antelación para asegurarse de que cualquier equipo o suministro pueda reemplazarse oportunamente.

Cuando ha ocurrido un desastre o 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 las noticias a través de otro canal. El DRP debe detallar cualquier guía para el manejo de la prensa. El sitio de la conferencia de prensa de emergencia debe planificarse con anticipación.

Al reanudar las operaciones normales después de un evento perturbador, 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 los daños que ocurren como resultado del evento. Además, deben adoptarse las medidas apropiadas para evitar nuevos daños a la propiedad.

El punto en común entre todos los planes de recuperación es que todos se vuelven obsoletos. Por esta razón, requieren pruebas y actualizaciones.

En esta sección se incluye un análisis de la categorización de las prioridades de recuperación de activos, la recuperación de procesos medioambientales, la recuperación de instalaciones, la recuperación de suministros y tecnología, la recuperación del entorno de usuario, la recuperación de datos y la capacitación del personal.

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 el objetivo de 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 un RPO estipula la cantidad de datos que una organización puede perder cuando se produce un desastre. Los valores de RTO, WRT y RPO se derivan durante el proceso BIA.

Al desarrollar la estrategia de recuperación, el comité del plan de recuperación toma el valor de RTO, WRT y RPO y determina las estrategias de recuperación que se deben usar para garantizar que la organización cumpla con 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 los sistemas que la mayoría de los sistemas críticos no se pueden restaurar utilizando métodos manuales. El comité del plan de recuperación debe comprender las soluciones de copia de seguridad y restauración que están disponibles e implementar el sistema que proporcionará la recuperación dentro de los valores de 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 de Negocios

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

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 bases de datos, el DRP debe incluir el servidor de bases de datos como un activo crítico. Aunque puede que no sea necesario restaurar toda la granja de servidores de bases de datos para restaurar el sistema de cuentas crítico, al menos uno de los servidores de la granja es necesario para el correcto funcionamiento.

Los documentos de flujo de trabajo se deben proporcionar 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 los roles y recursos necesarios del proceso, las herramientas de entrada y salida y las interfaces con otros procesos empresariales.

Suministro y recuperación de tecnología

Aunque la recuperación de las instalaciones no suele ser una preocupación por desastres más pequeños o eventos perturbadores, casi todos los esfuerzos de recuperación generalmente

implican la recuperación de suministros y tecnología. Las organizaciones deben asegurarse de que cualquier DRPs 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 deban comprar nuevos suministros y activos tecnológicos.

El DRP debe incluir información de recuperación en los siguientes activos que se deben restaurar:

- 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 se debe incluir 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 de cada uno de estos dispositivos, sino también información sobre la restauración manual de estos sistemas si los sistemas están dañados o completamente destruidos. También se deben identificar 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 deban explorar otras opciones, incluida la compra de sistemas redundantes y su 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 todos los sistemas operativos, bases de datos y utilidades que deben ejecutarse en el dispositivo.

Muchas organizaciones pueden pensar que este requisito se cumple si tienen una copia de seguridad en cinta, DVD, unidad flash, disco duro u otro medio de todo su software. Pero todo el software que se copia de seguridad por lo general requiere al menos un sistema operativo para ejecutarse 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 la 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 involucrados.

En muchos casos, las aplicaciones se adquieren a un proveedor de software y sólo el proveedor de software entiende la codificación que se produce en las aplicaciones. Dado que no hay garantías en el mercado actual, algunas organizaciones pueden decidir que necesitan asegurarse de que están protegidos contra la desaparición de un proveedor de software. Un depósito de garantía de software es un acuerdo por el cual se le da a un tercero el código fuente del software para garantizar que el cliente tenga acceso al código fuente si se producen ciertas condiciones para el proveedor de software, incluida la bancarrota y el desastre.

Recursos humanos

Ninguna organización es capaz de operar sin personal. Un plan de emergencia para ocupantes aborda específicamente los procedimientos para minimizar la pérdida de vidas o lesiones cuando ocurre una amenaza. El equipo de recursos humanos es responsable de ponerse en contacto con todo el personal en caso de desastre. La información de contacto de todo el personal debe almacenarse en el sitio 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 solo después de que el personal esté a salvo.

Después de que el evento inicial haya terminado, el equipo de recursos humanos debe monitorear 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 miembros del personal durante el proceso de recuperación. Cualquier DRP debe tener en cuenta la necesidad de proporcionar períodos adecuados de descanso para cualquier personal involucrado en el proceso de recuperación ante desastres. También debería incluir directrices sobre cómo reemplazar a cualquier personal que sea víctima del desastre.

La organización debe asegurarse de que los salarios y otros fondos para el personal continúen durante y después del desastre. Debido a que el financiamiento puede ser crítico tanto para el personal como para las compras de recursos, los cheques autorizados y firmados deben almacenarse de forma segura fuera del sitio. La administración de nivel inferior con los controles de acceso adecuados debe tener la capacidad de dispersar los fondos utilizando estos controles 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 los pasos apropiados para protegerse y continuar funcionando.

Suministros

A menudo, los desastres afectan la capacidad de suministrar a una organización los recursos necesarios, incluidos el papel, el cableado e incluso el agua. La organización debe documentar cualquier recurso que sea vital para sus operaciones diarias y los proveedores de los que se pueden obtener estos recursos. Debido a 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 implicado 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 de la organización que decida qué documentación departamental se necesita para llevar a cabo las operaciones cotidianas. Esta documentación debe almacenarse en una ubicación central en el sitio, y una copia debe conservarse fuera del sitio también. El personal específico debe tener la tarea de garantizar que esta documentación se cree, almacene y actualice según corresponda.

Recuperación del entorno de 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 al usuario final. Los usuarios deben ser notificados de dónde y cuándo informar después de que ocurra un desastre.

La recuperación del entorno de usuario real debe producirse en etapas, con las funciones más críticas que se restauran primero. Los requisitos del usuario deben documentarse para garantizar que se restauren todos los aspectos del entorno del usuario. Por ejemplo, es posible que todos los usuarios de un departamento crítico necesiten su propio equipo cliente. Es posible que estos mismos usuarios también necesiten tener acceso a una aplicación que se

encuentra en un servidor. Si no se restaura el servidor, los usuarios no podrán realizar sus tareas de trabajo 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 somos tan dependientes de la tecnología hoy en día, a menudo pasamos por alto los métodos manuales para realizar nuestras tareas de trabajo. La documentación de estos métodos manuales puede garantizar que las operaciones puedan seguir produciéndose, incluso si se producen a una velocidad disminuida.

Recuperación de datos

En la mayoría de las organizaciones, los datos son uno de los activos más críticos cuando se recuperan de un desastre. Los BSP y DRPs deben incluir directrices y procedimientos para la recuperación de datos. Sin embargo, los equipos de operaciones deben determinar de qué datos se realiza una copia de seguridad, con qué frecuencia se realiza la copia de seguridad de los datos y el método de copia de seguridad utilizado. Por lo tanto, mientras en esta sección se describe la copia de seguridad de datos, recuerde que los equipos bcp no toman realmente 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 una copia de seguridad se puedan restaurar de manera oportuna.

En esta sección se describen los tipos y esquemas de copia de seguridad de datos que se utilizan, 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 vivo.

PuntoClave18

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
- Copia de seguridad diferencial
- Backup incremental

- Copia de seguridad
- Copia de seguridad diaria
- Copia de seguridad del registro de transacciones
- Esquema de rotación de primero en entre y primero en salir
- Esquema 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, se habilita el bit de archivo para el archivo. 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 completo, se borra el bit de almacenamiento de 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 se debe 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 almacenamiento para cada archivo no se borra. Una copia de seguridad diferencial puede variar desde tomar poco 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 entonces. En una organización que usa un esquema completo/diferencial, se debe restaurar la copia de seguridad completa y solo la copia de seguridad diferencial más reciente, lo que significa que solo se necesitan dos copias de seguridad.

Una copia de seguridad incremental realiza 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 almacenamiento de cada archivo. Una copia de seguridad incremental suele tardar 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 el domingo y una copia de seguridad incremental todos los días 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

La tabla consta de cinco columnas y tres filas. Los encabezados de columna leen Tipo de copia de seguridad, Copia de seguridad de datos, Tiempo de copia de seguridad, Tiempo de restauración y Espacio de almacenamiento. La fila 1 dice: Copia de seguridad completa, Todos los datos, Más lento, Gordo y Alto. La fila 2 lee: Copia de seguridad incremental, Solo archivos o carpetas nuevos/modificados, Rápido, Moderado y Más bajo. La fila 3 dice: Copia de seguridad diferencial, Todos los datos desde la última vez que se completa, Moderado, Rápido y Moderado.

Figura 7-10 Comparación de tipos de copia de seguridad

Copia y copias de seguridad diarias son dos tipos de copia de seguridad especiales que no se consideran parte de ningún esquema de copia de seguridad programada regularmente porque no requieren ningún otro tipo de copia de seguridad para la restauración. Las copias de seguridad son similares a las copias de seguridad normales, pero no restablecen el bit de almacenamiento del archivo. Las copias de seguridad diarias utilizan la marca de tiempo de un archivo para determinar si necesita archivado. 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 en los que 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 utilizan con mayor frecuencia en entornos de bases 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 realizan una copia de seguridad de sus datos en discos ópticos, incluidos CD-ROM, DVD y discos Blu-ray; accionamientos magnéticos de alta capacidad y alta velocidad; medios basados en flash; u otros medios. Independientemente de los medios utilizados, es importante conservar las copias de seguridad tanto en el sitio como fuera del sitio. Guarde las copias de seguridad en el sitio en una caja fuerte o bóveda impermeable, resistente al calor y resistente al fuego.

Copia de seguridad electrónica

Las soluciones de copia de seguridad electrónica realizan copias de seguridad de los 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 los archivos a medida que se producen modificaciones. Este método se produce en tiempo real.
- **Registro en diario remoto:** Copia el diario o el registro de transacciones fuera del sitio según una programación regular. Este método se produce en lotes.
- **Bóveda de cintas:** 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.
- **Administración jerárquica del almacenamiento (HSM):** Almacena los datos a los que se accede con frecuencia en medios más rápidos y los datos a los que se accede con menos frecuencia en medios más lentos.
- **Jukebox óptico:** Almacena datos en discos ópticos y utiliza robótica para cargar y descargar los discos ópticos según sea necesario. Este método es ideal cuando se requiere disponibilidad 24/7.
- **Replicación:** Copia datos de una ubicación de almacenamiento a otra. La replicación sincrónica utiliza actualizaciones de datos constantes para asegurarse de que las ubicaciones están cerca de las mismas, mientras que la replicación asincrónica retrasa las actualizaciones a una programación predefinida.

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

Capacitación del personal

Incluso si una organización toma las medidas para desarrollar los BCPs y DRPs más exhaustivos, 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. El personal debe disponer del tiempo y los recursos monetarios adecuados para garantizar que se imparta una formación adecuada. Esto incluye permitir que el personal pruebe cualquier DRPs.

La capacitación debe obtenerse de fuentes internas y externas. Cuando los deberes del trabajo cambian o se contrata a nuevo personal, las políticas deben estar en el lugar para asegurar la transferencia apropiada del conocimiento ocurre.

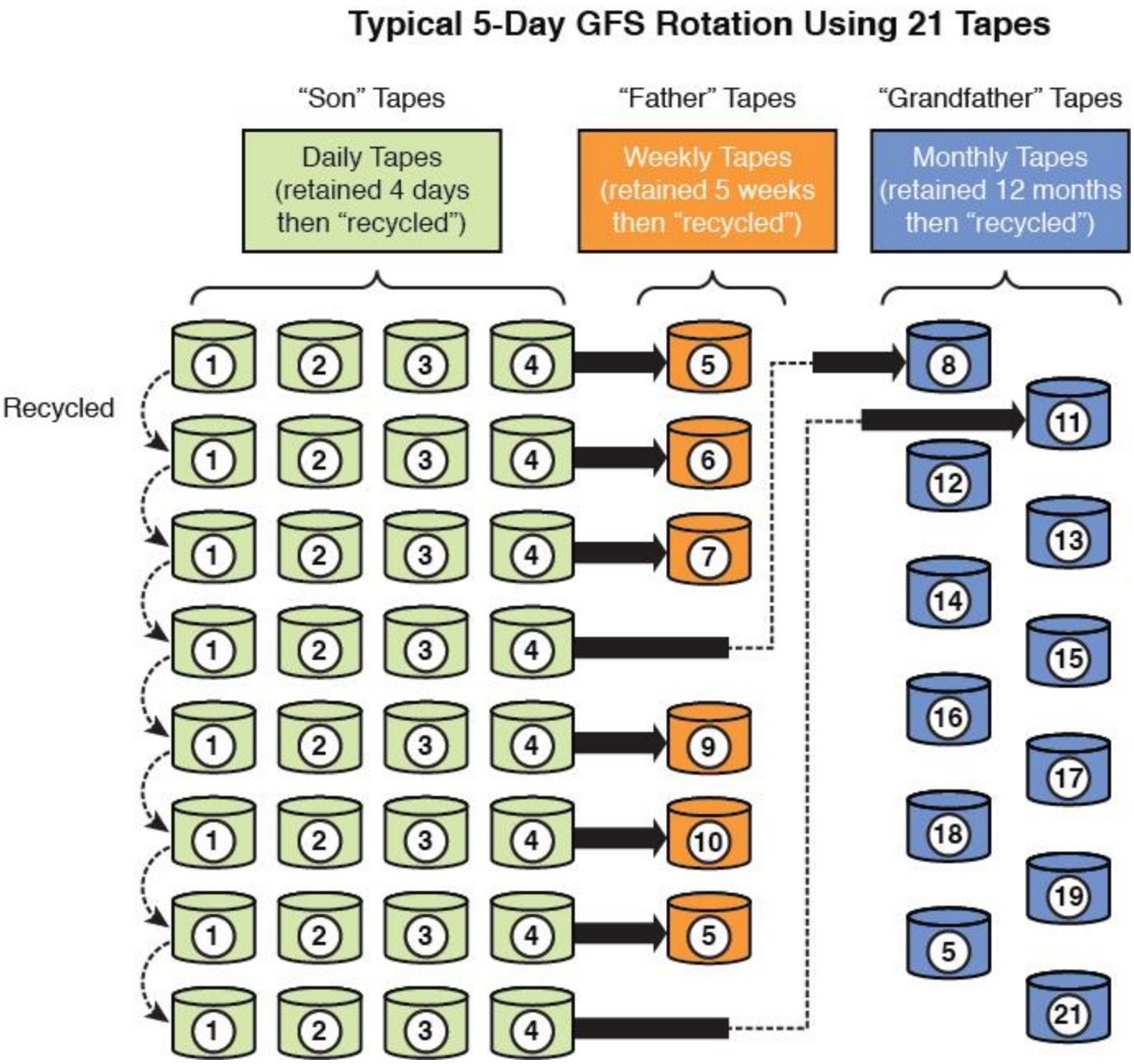
Estrategias de almacenamiento de información de backup

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 utilizará. Las consideraciones de costo 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 se planifica de antemano, los medios pueden volverse poco confiables debido al uso excesivo. Dos de los esquemas de rotación de respaldo más populares son primero en salir, primero en salir y abuelo / padre / hijo.

En el esquema FIFO (primero en iniciar, primero en salir), 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, las copias de seguridad semanales son los padres, y las copias de seguridad mensuales son los abuelos. Cada semana, un hijo avanza al conjunto paterno. Cada mes, un padre avanza al conjunto del abuelo.

La Figura 7-11 muestra una rotación típica de GFS de 5 días utilizando 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.



Las Cintas "Son" con una caja que dice, Cintas Diarias (conservadas 4 días luego recicladas) muestran cuatro cilindros marcados 1,2,3, y 4, apilados en ocho capas de arriba a abajo. Una flecha con la etiqueta "Reciclado" fluye desde la capa superior a las capas consecutivas. Las Cintas Father con una caja que dice, Cintas Semanales (conservadas 5 semanas y luego recicladas) muestra 6 cilindros dispuestos verticalmente y marcados 5, 6, 7, 9, 10 y 5, respectivamente. Las cintas del abuelo con una caja que lee cintas mensuales (conservadas 12 meses y luego recicladas) tiene dos juegos de cilindros dispuestos verticalmente. El primer conjunto está marcado como 8, 12, 14, 16, 18 y 5. El segundo conjunto está marcado como 11, 13, 15, 17, 19 y 21. Las flechas del cilindro marcadas cuatro en las capas primera, segunda, tercera, quinta, sexta y séptima" de las Cintas Son apuntan a los cilindros correspondientes de

la Capa Padre. Las flechas de los cilindros marcados 4 de las capas cuatro y ocho de las cintas son apuntan al cilindro 8 y 11, respectivamente, en las cintas del abuelo.

Figura 7-11 Esquema de rotación de respaldo abuelo/padre/hijo

Estrategias de recuperación y 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 restaure 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 regresará de la ubicación alternativa a la instalación principal después de que se restaure. Además, por motivos de seguridad, el DRP debe incluir detalles sobre los controles de seguridad que se utilizaron 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 del DRP es asegurarse de que la ubicación alternativa no se vea afectada por el mismo desastre. Esto podría significar que la organización debe seleccionar una ubicación alternativa que se encuentra en otra ciudad o región geográfica. Los principales factores que afectan a la selección de una ubicación alternativa son los siguientes:

- Ubicación geográfica
- Necesidades de la organización
- 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 DRP debe incluir instrucciones sobre cuándo y cómo probar periódicamente las instalaciones alternativas para garantizar que la instalación de contingencia sea compatible con la instalación primaria.

Las ubicaciones alternativas que los profesionales de la 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 pocas horas para llevar un sitio caliente a la operación completa.

Aunque un sitio activo proporciona la recuperación más rápida, es el más costoso 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 redundancia completa, incluido el hardware, el software y el cableado de comunicación.

Sitio frío

Un sitio frío es una instalación arrendada que contiene solo cableado eléctrico y de comunicaciones, aire acondicionado, plomería y pisos elevados. No se instala ningún equipo de comunicaciones, hardware de red o equipos en un sitio frío hasta que sea necesario poner el sitio en pleno 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 se incluyen en un sitio caliente son los equipos. Un sitio caliente 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 un sitio frío. Es la ubicación arrendada alternativa más ampliamente implementada. Aunque probar un sitio caliente es más fácil que probar un sitio frío, un sitio cálido requiere mucho más esfuerzo para probar que un sitio caliente.

La figura 7-12 es un gráfico que compara los componentes implementados en estos tres sitios.

PuntoClave19

Key Topic

	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

Se muestran cuatro columnas y cinco filas. Los encabezados de fila leen Hot Site, Warm Site, Cold Site. La fila 1 lee Conexión eléctrica, Sí, Sí y Sí. La fila 2 lee Periféricos, Sí, Algunos y Ninguno. La fila 3 lee Redes, Sí, Ninguno y Ninguno. La fila 4 lee Servidores y otro hardware, Sí, Ninguno y Ninguno. La fila 5 lee Aplicaciones, Sí, Ninguno y Ninguno.

Figura 7-12 Comparación de sitios calientes, sitios calientes y sitios fríos

Sitio Terciario

Un sitio terciario es un sitio de copia de seguridad secundario que proporciona una alternativa en caso de que el sitio caliente, el sitio caliente o el sitio frío no estén disponibles. Muchas grandes empresas implementan sitios terciarios para protegerse contra catástrofes que afectan a grandes áreas geográficas.

Por ejemplo, si una organización requiere un centro de datos que se encuentra en la costa, la organización podría tener su ubicación principal en Nueva Orleans, Luisiana, y su sitio caliente en Mobile, Alabama. Esta organización podría considerar la posibilidad de localizar un sitio terciario en Omaha, Nebraska, porque un huracán puede afectar tanto a la costa de Luisiana como a la costa del Golfo de Alabama.

Acuerdos recíprocos

Un acuerdo recíproco es un acuerdo entre dos organizaciones que tienen necesidades tecnológicas e infraestructuras similares. En el acuerdo, ambas organizaciones acuerdan actuar como un lugar alternativo para la otra si cualquiera de las instalaciones principales de la organización queda inutilizable. Lamentablemente, en la mayoría de los casos, estos acuerdos no pueden aplicarse legalmente.

Una desventaja de este sitio es que es posible que no sea capaz de controlar la carga de trabajo y las operaciones necesarias de la otra organización.

Nota

Un acuerdo de ayuda mutua es un acuerdo preestablecido entre dos organizaciones en el que cada organización se compromete a prestar asistencia a la otra en caso de desastre.

Sitios redundantes

Un sitio redundante o reflejado es un sitio que está configurado de forma idéntica que el sitio primario. Un sitio redundante o reflejado no es un sitio arrendado, sino que normalmente es propiedad de la misma organización que el sitio primario. La organización es responsable de mantener el sitio redundante. Varios sitios de procesamiento también se pueden configurar para que sirvan como sitios con redundancia operativa.

Aunque los sitios redundantes son costosos de mantener, muchas organizaciones hoy en día los ven como un gasto necesario para garantizar que se pueda proporcionar un servicio ininterrumpido.

Sistemas, instalaciones y alimentación redundantes

En previsión de desastres y eventos disruptivos, las organizaciones deben implementar redundancia para sistemas, instalaciones y energía críticos y evaluar cualquier sistema que se haya identificado como crítico para determinar si la implementación de sistemas redundantes es rentable. La implementación de sistemas redundantes en una ubicación alternativa a menudo garantiza que los servicios sean ininterrumpidos. Los sistemas redundantes incluyen servidores redundantes, enrutadores redundantes, hardware interno redundante e incluso redes troncales redundantes. La redundancia se produce cuando una organización tiene un componente secundario, sistema o dispositivo que se hace cargo cuando se produce un error en la unidad principal.

Las instalaciones redundantes garantizan que la organización mantenga una instalación en el nivel que elija para garantizar que los servicios de la organización puedan continuar cuando se produzca un evento disruptivo. Las instalaciones redundantes se examinan con más detalle en otras partes de este capítulo.

La redundancia de energía se implementa utilizando fuentes de alimentación ininterrumpidas (UPS) y generadores de energía.

También se puede proporcionar redundancia en componentes individuales. Los componentes de repuesto son repuestos fríos, repuestos calientes o hot spares. Un repuesto en frío no está encendido, pero se puede insertar en el sistema si es necesario. Un repuesto caliente está en el

sistema, pero no tiene energía a menos que sea necesario. Un hot spare está en el sistema y encendido, listo para estar operativo en cualquier momento.

Tecnologías de tolerancia a fallos

La tolerancia a fallos permite que un sistema continúe funcionando en caso de fallo de uno o más componentes. La tolerancia a errores dentro de un sistema puede incluir tarjetas adaptadoras tolerantes a fallos y unidades de almacenamiento tolerantes a fallos. Uno de los sistemas de tolerancia a fallos más conocidos es RAID, que se ha tratado 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 fallos, el seguro no es realmente una medida preventiva. Si una organización compra un seguro para proporcionar protección en caso de un evento perturbador, el seguro no tiene poder para proteger contra el evento en sí. El propósito del seguro es asegurar que la organización tenga 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 aún podrían quedarse cortas cuando la recuperación real debe tener lugar. Al comprar un seguro, la organización puede asegurarse de que las transacciones financieras clave, incluidas la nómina, las cuentas por pagar y los costos de recuperación, estén cubiertos.

La valoración del costo real del seguro (ACV) compensa la propiedad en función del valor del artículo en la fecha de la pérdida más el 10 por ciento. Sin embargo, tenga en cuenta que el seguro sobre cualquier material impreso solo cubre documentos, manuscritos o registros inscritos, impresos o escritos. No cubre el dinero y los valores. Un tipo especial de seguro llamado seguro de *interrupción del negocio* proporciona protección monetaria para los gastos y la 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 prevención contra el evento disruptivo. Todas las organizaciones deben asegurarse de que

todos los sistemas que almacenan archivos importantes se copian de manera oportuna. También se debe alentar 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 que se puedan restaurar los archivos.

La recuperación de datos, incluidos los tipos y esquemas de copia de seguridad y la copia de seguridad electrónica, se trataron 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.

Entre los términos y técnicas de alta disponibilidad que debe comprender se 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 rápidamente disponibles desde los discos restantes de la matriz sin restaurar desde una cinta de copia de seguridad u otro medio 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 de 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 clúster, una instancia de un servidor de aplicaciones actúa como controlador maestro y distribuye las solicitudes a varias instancias utilizando algoritmos round robin, weighted round robin o least-connections.
- **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 usan procesos complejos de reducción de

números, como la utilización de cpu y memoria por servidor, los 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 de servidores.

Calidad de servicio

La calidad de servicio (QoS) es una tecnología que administra los recursos de red para garantizar un nivel de servicio predefinido. Asigna prioridades de tráfico a los diferentes tipos de tráfico o protocolo en una red. QoS implementa cuando ocurre 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 proporciona el administrador. La importancia se puede basar en la dirección IP, la dirección MAC, e incluso el nombre del servicio. Sin embargo, QoS trabaja solamente cuando ocurre un cuello de botella en la ubicación apropiada y las configuraciones son sus declaraciones de ancho de banda. Por ejemplo, si las configuraciones de QoS se fijan más allá del ancho de banda ISP, el tráfico no será dado prioridad si un router piensa que hay bastante ancho de banda disponible. Pero, ¿qué pasa si se cumplen los máximos del ISP y el ISP decide qué es o no importante? La clave para cualquier implementación de QoS es ajustar la configuración y observar la red a lo largo del tiempo.

Resistencia del sistema

La resiliencia del sistema es la capacidad de un sistema, dispositivo o centro de datos para recuperarse rápidamente y continuar funcionando después de una falla 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 se hace cargo sin problemas y continúa proporcionando servicios a los usuarios.

7.10 Recuperación ante desastres

La recuperación ante desastres implica la restauración de servicios y sistemas desde un estado de contingencia, o el estado temporal en el que pueden estar las operaciones donde se están ejecutando, pero no en la instalación principal o en los recursos óptimos. El DRP se analiza 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 concientización.

Respuesta

Una vez que se ha producido un evento, se debe contactar con el personal apropiado para iniciar las comunicaciones que alertan al equipo de recuperación apropiado y al personal afectado del evento. Todos los equipos enumerados en la sección de personal deben

desempeñar sus funciones. Se debe desarrollar una jerarquía de procesos para que cada equipo realice sus tareas como parte del proceso de recuperación ante desastres en el orden correcto.

Personal

Aunque las prioridades número uno y número dos cuando ocurre un desastre son la seguridad del personal y la salud y la mitigación de daños, respectivamente, la recuperación de un desastre se convierte rápidamente 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 asegurarse de que el personal puede realizar sus tareas durante la recuperación ante desastres, debe conocer y comprender sus tareas de trabajo.

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

Las organizaciones deben decidir qué equipos son necesarios durante una recuperación ante desastres y asegurarse de que se coloca el personal adecuado 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 necesiten 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 de comunicación
- 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 daños que se han producido en 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 deberán restaurarse y reemplazarse y se pone en contacto con los equipos apropiados que deben activarse.

Equipo Legal

El equipo legal se ocupa de todos los problemas legales inmediatamente después del desastre y durante la recuperación ante desastres. El equipo legal supervisa cualquier evento de relaciones públicas que se lleva a cabo 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 asegurarse de 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 DRP. El sitio de la conferencia de prensa de emergencia debe planificarse con anticipación. Al emitir declaraciones públicas, el equipo de relaciones con los medios 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 ser unificada.

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 de comunicación lo descubren a través de otro canal. Cualquiera que haga anuncios de desastres al público debe entender que la audiencia de tales anuncios incluye a los medios de comunicación, los sindicatos, las partes interesadas, los vecinos, los empleados, los contratistas e incluso los competidores.

Equipo de recuperación

La tarea principal del equipo de recuperación es recuperar las funciones críticas del negocio en la instalación alternativa. Esto implica principalmente asegurarse de que los activos físicos están en su lugar, incluidos los equipos y otros dispositivos, el 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 primario esté listo para funcionar.

Equipo de Restauración

El equipo de restauración realmente se asegura de que los activos y los datos se restauren a 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 garantiza que el sitio primario vuelva a la normalidad. El equipo de salvamento gestiona la limpieza de los equipos, supervisa la reconstrucción de la instalación original e identifica a los expertos que se emplear en el proceso de recuperación. En la mayoría de los casos, el equipo de salvamento 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 a menudo es mucho más grande, es posible que el equipo de seguridad deba 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 son mejores 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 de manera oportuna. También es importante asegurarse de que no se omite ningún paso y que los pasos se producen en el orden correcto. La comunicación con el personal depende de quién está siendo contactado sobre el desastre. El personal que se ve afectado por un desastre debe recibir comunicaciones que enumeremos 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 ocurre un evento, el personal necesita evaluar la gravedad y el impacto del evento. Al hacerlo, se garantiza que se implementa la respuesta adecuada. La mayoría de las organizaciones establecen categorías de eventos, incluidos los que no son incidentes, incidentes e incidentes graves. Cada organización debe tener un proceso de evaluación de recuperación ante desastres para garantizar que el personal evalúe correctamente cada evento.

Restauración

El proceso de restauración implica la restauración de los sistemas e instalaciones primarias a su funcionamiento normal. El personal involucrado en este proceso depende de los activos que se vieron afectados por el evento. Todos los equipos que participen en la recuperación de activos deben 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 bases de datos estén operativos, el administrador de bases de datos debe trabajar estrechamente con el administrador de la aplicación web para asegurarse de que ambos vuelven a funcionar normalmente.

Formación y sensibilización

El personal de todos los niveles debe recibir la capacitación adecuada sobre el proceso de recuperación en casos de desastre. Los usuarios habituales solo necesitan recibir capacitación en sensibilización 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 la logística. Los profesionales de la seguridad necesitan formación sobre cómo proteger los activos durante la recuperación.

La mayoría de las organizaciones incluyen capacitación sobre continuidad del negocio y concientización sobre recuperación ante desastres como parte de la capacitación inicial que se otorga al personal cuando es contratado. Las organizaciones también deben actualizar periódicamente al personal para asegurarse de que no se olvidan de la recuperación ante desastres.

Nota

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

7.11 Probar planes de recuperación ante desastres

Después de que el BCP esté completamente documentado, una organización debe tomar medidas para garantizar que el plan se mantenga y se mantenga actualizado. Como mínimo, una organización debe evaluar y modificar el BCP y el DRP anualmente. Esta evaluación generalmente implica algún tipo de prueba para garantizar 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 la prueba. A través de las pruebas, se detectan inexactitudes, deficiencias y omisiones.

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

PuntoClave20

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

- Prueba de lectura a través
- Prueba de lista de comprobación
- Ejercicio de mesa
- Prueba de recorrido estructurada
- Prueba de simulación
- Prueba paralela
- Prueba de interrupción completa
- Taladro funcional
- Taladro de evacuación

Prueba de lectura a través

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 comprobación

La prueba de lista de comprobación se produce cuando los administradores de cada departamento o área funcional revisan el BCP. Estos gerentes hacen notar cualquier

modificación al plan. A continuación, el comité bcp utiliza todas las notas de administración para realizar cambios en el BCP.

Ejercicio de mesa

Un ejercicio de mesa es la forma más rentable y eficiente de identificar las 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 acuerdan un escenario de desastre particular en el que se centrarán.

Prueba de recorrido estructurada

La prueba de recorrido estructurado implica que representantes de cada departamento o área funcional revisen a fondo la precisión del BCP. Este tipo de prueba es la prueba más importante para realizar antes de un desastre en vivo.

Prueba de simulación

En una prueba de simulación, el personal de operaciones y soporte ejecuta 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 manteniendo las operaciones en el sitio primario.

Prueba de interrupción completa

Una prueba de interrupción completa implica el cierre de la instalación primaria y llevar la instalación alternativa a la operación completa. Se trata de un cambio duro en el que todo el procesamiento se produce en la instalación principal hasta que se lanza el "conmutador". Este tipo de prueba requiere una coordinación completa entre todas las partes e incluye la notificación a los usuarios con antelación de la prueba prevista. Una organización debe realizar este tipo de prueba solo cuando todas las demás pruebas se han implementado y se han 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.

Taladro de evacuación

En un simulacro de evacuación, el personal sigue las pautas de evacuación o refugio en el lugar para un tipo de desastre en particular. En este tipo de simulacros, el personal debe entender el área a la que deben reportar cuando se produzca la evacuación. Todo el personal debe ser contabilizado en ese momento.

Planificación y ejercicios de continuidad del negocio

Una vez completada una prueba, se deben documentar todos los resultados de la prueba y los planes deben modificarse para reflejar esos resultados. La lista de actividades correctas y no exitosas de las pruebas será la más útil para la administración al mantener el BCP. Toda la información obsoleta en los planes debe ser eliminada, y cualquier información nueva debe ser agregada. Además, podría ser necesario modificar la información actual en función de las nuevas regulaciones, leyes o protocolos.

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

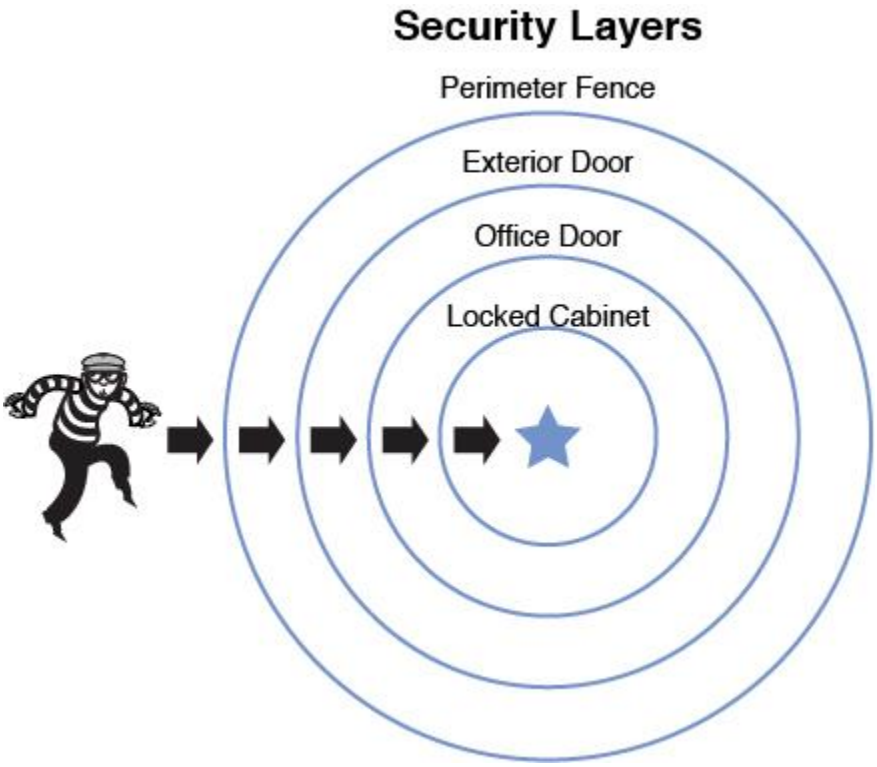
7.12 Seguridad física

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 perimetral apropiados, incluyendo puertas y cercas, detección de intrusiones perimetrales, iluminación, fuerza de patrulla 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 seguridad internos y de construcción adecuados.

PuntoClave21

Controles de seguridad perimetral

Al considerar la seguridad perimetral de una instalación, adoptar 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.



Cuatro círculos concéntricos representan las cuatro capas de seguridad. El círculo más interno con una estrella se etiqueta gabinete bloqueado. El círculo junto a él está etiquetado como Puerta de la Oficina. La siguiente capa tiene la etiqueta Puerta exterior. La capa más externa tiene la etiqueta Valla perimetral. Un ladrón intenta acercarse a la estrella en el centro, pero tiene que cruzar estos anillos de seguridad; su trayectoria de aproximación a la estrella central se muestra mediante flechas.

Figura 7-13 Enfoque del círculo concéntrico

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

Puertas y cercas

El anillo más externo en el enfoque de círculo concéntrico se compone de las puertas y vallas que rodean la instalación. Dentro de eso hay círculos interiores de barreras físicas, cada una de las cuales tiene su propio conjunto de preocupaciones. En esta sección, se cubren las consideraciones para barreras (bolardos), cercas, puertas y paredes.

Barreras (Bolardos)

Las barreras llamadas *bolardos* se han vuelto bastante comunes alrededor del perímetro de los nuevos edificios de oficinas y gubernamentales. Estos son postes verticales cortos colocados en el camino de entrada del edificio y que recubren las aceras que ayudan a proporcionar protección contra los vehículos que podrían chocar intencionalmente o no, o entrar en el edificio o lesionar a los peatones. Pueden estar hechos 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 cercado a 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 solo disuaden a los intrusos ocasionales.
- Las vallas de 6 a 7 pies de altura son demasiado altas para escalar fácilmente.
- Las cercas de 8 pies y más altas disuaden a los intrusos más determinados, especialmente cuando se aumentan con alambre de afeitar.

Una geo-cerca es un área geográfica dentro de la cual los dispositivos se gestionan utilizando algún tipo de comunicación por radiofrecuencia. Por ejemplo, una geo-cerca se podría configurar 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 realizar un seguimiento de los usuarios o dispositivos que entran o salen del área de geo-cerca. Las alertas se pueden configurar para enviar un mensaje al usuario del dispositivo y al operador de geo-cerca de la ubicación del dispositivo.

Portones

Las puertas pueden ser puntos débiles en una cerca si no se manejan correctamente. Las puertas son calificadas 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, las paredes pueden ser llamadas 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 analizan a continuación, se pueden implementar para avisarle de cualquier violación de las paredes.

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 de infrarrojos pasivos (PIR) funcionan identificando cambios en las olas 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 hace sonar una alarma cuando esto ocurre.

Sistemas Electromecánicos

Los sistemas electromecánicos funcionan detectando una rotura en un circuito eléctrico. Por ejemplo, el circuito puede cruzar una ventana o puerta y cuando se abre la ventana o puerta, el circuito se rompe, 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 del área, y si el haz es interrumpido (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 solo 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 perturbe el patrón de onda. Cuando se altera el patrón, 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, sonará la alarma.

CCTV

Un sistema de circuito cerrado de televisión (CCTV) utiliza conjuntos de cámaras que se pueden monitorear en tiempo real o pueden grabar 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 de usar CCTV es que aumenta las capacidades visuales del guardia. Los guardias pueden monitorear áreas más grandes a la vez desde una ubicación central. Cctv es una categoría de vigilancia física, no de vigilancia informática / red.

Los tipos de cámaras incluyen cámaras para exteriores, 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, la resolución, los fotogramas por segundo (FPS) y la compresión adecuados. Además, se debe entender el análisis de los requisitos de iluminación de las diferentes cámaras; un sistema de CCTV debe funcionar en la cantidad de luz que proporciona la ubicación. Además, una organización debe comprender los diferentes tipos de pantallas de monitor, incluidas las pantallas de una sola imagen, pantalla dividida y de gran formato.

Iluminación

Una de las mejores maneras de disuadir el crimen y la travesura es arrojar luz sobre las áreas de preocupación. En esta sección, analizamos algunos tipos de iluminación y algunos sistemas de iluminación que han demostrado ser efectivos. 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 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 apagó la energía

Tipos de iluminación

Hay varias opciones 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 de vapor de mercurio de muy baja presión que utiliza la 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 un 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 fundida que transmite luz ultravioleta con poca absorción.

Independientemente de la fuente de luz, será calificado por sus *pies de iluminación.* Al colocar las luces, debe tener en cuenta esta calificación. Por ejemplo, si una luminaria controlada montada en un poste de 5 metros puede iluminar un área de 30 metros de diámetro, por motivos de iluminación de seguridad, la distancia entre las luminarias debe ser de 30 pies. Además, debe haber una amplia iluminación perimetral exterior de las entradas o áreas de estacionamiento para desalentar a los merodeadores o intrusos ocasionales.

Fuerza de Patrulla

Un excelente aumento para todos los demás sistemas de detección es la presencia de un guardia que patrulla la instalación. Esta opción ofrece la mayor flexibilidad para reaccionar ante lo que ocurra. Una de las claves del éxito es la adecuada formación 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 usar 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 por contrato. Una organización puede controlar el entrenamiento 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, se deben seguir una serie de directrices con respecto al mantenimiento de registros. Todo intento exitoso y fallido de ingresar a la instalación, incluidos los casos en que se concedió la admisión, debe registrarse de la siguiente manera:

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

Controles de construcción y seguridad interna

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

7.13 Seguridad y protección del personal

Los recursos humanos son los activos más importantes que posee la organización. Tal vez recuerde que en caso de incendio, la primera acción a tomar siempre es evacuar a todo el personal. Su seguridad está por delante de 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 para Ocupantes (OEP, por sus sus, por sus, por sus, por sus contra ocupantes) proporciona procedimientos coordinados para minimizar la pérdida de vidas o lesiones y proteger los daños a la propiedad 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 necesariamente y por lo general no se extiende a sus actividades en la red, tanto las leyes federales como las estatales responsabilizan a las organizaciones por la divulgación de este tipo de información, con violaciones que resultan en fuertes multas y posibles demandas si la compañía es declarada responsable.

Las organizaciones deben desarrollar políticas para lidiar con la coacción de los empleados, los viajes, el monitoreo, la gestión de emergencias y la capacitación y concientización sobre seguridad.

Coacción

La coacción del empleado ocurre cuando un empleado es coaccionado a cometer una acción por 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 cualquier código de seguridad, PIN o contraseña que se utilice, es una buena política implementar un código de coacción secundario. Luego, si el personal está bajo coacción, utiliza el código de coacción para acceder a los sistemas, instalaciones u otros activos. El personal de seguridad es alertado de que se ha utilizado el código de coacción. Las organizaciones deben recalcar al personal 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 mantengan seguros los activos emitidos por la organización durante el período

de viaje y para tener especial cuidado cuando estén en público. También deben recibir instrucciones para informar adecuadamente sobre los activos perdidos o robados.

Monitorización

Es posible que sea necesario supervisar las acciones de los empleados en los activos de la organización, 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 monitorearán a los empleados deben emitir una declaración de no expectativa de privacidad. Los empleados deben recibir una copia de esta declaración cuando sean contratados y deben firmar un recibo de la declaración. Además, los recordatorios periódicos de esta política deben colocarse en lugares destacados, incluidos los tablones de anuncios, las pantallas de inicio de sesión y los sitios web.

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

Manejo de emergencias

Las organizaciones deben contar con políticas y procedimientos específicos de gestión de emergencias. Se deben formar equipos de manejo de emergencias para documentar los tipos de emergencias que podrían ocurrir y preparar los planes de emergencia apropiados para ser utilizados si ocurre una emergencia específica.

Estos planes deben ser probados periódicamente para asegurar que el personal entienda qué hacer en caso de una emergencia y revisados en función de los resultados de estas pruebas.

Las emergencias que deben anticiparse incluyen eventos climáticos (como tornados, huracanes y tormentas de invierno), 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. El manejo de emergencias se refiere a 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.

Capacitación y concientización sobre seguridad

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

Tareas de preparación del examen

Como se mencionó en la sección"Acerca de la *Guía de Certificados CISSP*,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 del examen en el Pearson Test Prep Software Online.

Revisar todos los temas clave

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

Cuadro 7-2 Temas clave para el capítulo 7

Elemento tema clave	Descripción	Número de página
Lista	Pasos de la 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 prueba	17°
Lista	Tipos de evidencia	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
Sección	Conceptos de operaciones de seguridad	593
Tabla 7-1	Niveles raid	20°
Lista	Pasos de respuesta a incidentes	610

Elemento tema clave	Descripción	Número de página
Párrafo	Medidas detectivescas y preventivas	612
Lista	Pasos del ciclo de vida de la administración de parches	617
Lista	Tipos y esquemas de copia de seguridad de datos	22°
Figura 7-12	Comparación de sitios calientes, sitios calientes y sitios fríos	629
Lista	Tipos de pruebas utilizadas para evaluar bcp y 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

regla de la mejor evidencia

Listas negras

Bolardos

cadena de custodia

evidencia circunstancial

investigación civil

Puerta de clase 1

Puerta de clase 2

Puerta de clase 3

Puerta de clase 4

niveles de recorte

sistema de circuito cerrado de televisión (CCTV)

sitio frío

pruebas concluyentes

análisis de contenido

copia de seguridad

evidencia corroborativa

escena del crimen

investigación criminal

copia de seguridad diaria

borrado de datos

software de prevención de pérdida de datos (DLP)

purga de datos

copia de seguridad diferencial

evidencia directa

imágenes de disco

control dual

coacción

supervisión de salida

detección electrónica (exhibición de documentos electrónicos)

bóveda electrónica

iluminación de emergencia

evento

conmutación por error

failsoft

tolerancia a fallos

pies de iluminación

primero en entre, primero en salir (FIFO)

fluorescente

copia de seguridad completa

prueba de interrupción completa

abuelo/padre/hijo (GFS)

pruebas de oídas

sistema de administración jerárquica de almacenamiento (HSM)

alta disponibilidad

honeynet

honeypot

hot site

incident

incremental backup

intangible assets

job rotation

least privilege

means

mercury vapor

motive

movable lighting

necesidad de saber

almacenamiento de información conectado en red (NAS)

investigación de operaciones

seguridad de las operaciones

evidencia de opinión

oportunidad

sistema de infrarrojo pasivo (PIR)

sistema fotométrico

calidad de servicio (QoS)

lámpara de cuarzo

prueba paralela

RAID 0

RAID 1

RAID 2

RAID 3

RAID 5

RAID 10

prueba de lectura a través

acuerdo recíproco

redundancia

sitio redundante

investigación regulatoria

remanencia

aprovisionamiento de recursos

análisis de causa de origen

espacio aislado

buscar

evidencia secundaria

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 de recorrido estructurado

vigilancia

resistencia del sistema

activos tangibles

sitio terciario

copia de seguridad del registro de transacciones

ruta de acceso de confianza

recuperación de confianza

control de dos personas

sitio cálido

listas blancas

Responder preguntas de revisión

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

1. Responder al incidente.
2. Detectar el incidente.
3. Denunifique 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 la evidencia?

1. Sea preciso.
2. Sé completo.
3. Ser admisible.
4. Sea volátil.

4. ¿Cuál de las siguientes se refiere a permitir a los usuarios el acceso sólo a los recursos necesarios para realizar su trabajo?

1. Rotación de puestos
2. Separación de funciones
3. Necesidad de saber/privilegios mínimos
4. Vacaciones obligatorias

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

1. Unidad de disco
2. Receta
3. Gente
4. Servidor

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

1. Detectar
2. Responder
3. Monitor

4. Informe

7. ¿Cuál de los siguientes 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 el pleno funcionamiento?

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. Jukebox óptico
2. Administración jerárquica del almacenamiento de información
3. Bóveda de cintas
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 error 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 de almacenamiento

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

1. Prevención de pérdida de datos (DLP)
2. Regulador
3. Exhibición de documentos electrónicos
4. Operaciones

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

1. Supervisión de salida
2. Monitorización continua
3. CMaaS
4. Aprovisionamiento de recursos

13. ¿Cuáles de los siguientes se consideran activos virtuales? (Elija todo lo que se aplique).)

1. Redes definidas por software
2. Redes de área de almacenamiento virtual
3. Sistemas operativos invitados implementados en máquinas virtuales
4. Enrutadores virtuales

14. ¿Cuál de las siguientes opciones describe la capacidad de un sistema, dispositivo o centro de datos para recuperarse rápidamente y continuar funcionando después de una falla del equipo, corte de energía u otra interrupción?

1. Calidad de servicio (QoS)
2. Objetivo de tiempo de recuperación (RTO)
3. Objetivo de punto de recuperación (RPO)
4. Resistencia 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 se aplique).)

1. Ubicación geográfica
2. Necesidades de la organización
3. Costo de la ubicación
4. Esfuerzo de restauración de la ubicación

16. ¿Cuál de las siguientes 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 pueden estar disponibles rápidamente desde 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 utilizar?

1. Registro del sistema
2. Registro de aplicación
3. Registro de firewall
4. Registro de cambios

18. ¿Qué debe realizar con toda la información aceptada en un sistema para asegurarse de que es del tipo de datos y el formato 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 se aplique).)

1. Quitar aplicaciones innecesarias.
2. Deshabilite los servicios innecesarios.
3. Bloquear puertos no adquiridos.
4. Controle estrechamente la conexión de dispositivos de almacenamiento externos y medios.

Respuestas y explicaciones

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

1. Detectar el incidente.
2. Responder al incidente.
3. Reporte el incidente al personal apropiado.
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 reglas de la prueba son las siguientes:

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

4.c. Al permitir el acceso a los recursos y asignar derechos para realizar operaciones, siempre se debe aplicar 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 debe ser sin acceso. Conceda a los usuarios acceso solo a los recursos necesarios para realizar su trabajo, y ese acceso debe requerir la implementación manual después de que un supervisor haya comprobado 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. Detectar el incidente.
2. Responder al incidente.
3. Mitigar el incidente.
4. Denunifique 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 respaldo.

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

9. a. Una jukebox óptica 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. La detección electrónica (eDiscovery) se refiere a litigios o investigaciones gubernamentales que tratan con el intercambio de información en formato electrónico como parte del proceso de descubrimiento. Involucra 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 el conocimiento de las acciones que se pueden y no se pueden tomar con respecto a un documento. Una investigación regulatoria ocurre cuando un organismo regulador investiga a una organización por una infracción regulatoria. Las investigaciones de operaciones involucran cualquier investigación que no resulte en ningún problema penal, civil o regulatorio. En la mayoría de los casos, este tipo de investigación se completa para determinar la causa raíz de modo 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 supervisión de salida se lleva a cabo mediante firewalls que supervisan 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 monitoreo debe ser parte de un programa de monitoreo continuo de la organización. El programa de monitoreo continuo debe estar diseñado para satisfacer las necesidades de la organización e implementado correctamente para garantizar que la infraestructura crítica de la organización esté vigilada. Es posible que las organizaciones deseen examinar las soluciones CMaaS implementadas por los proveedores de servicios en la nube. El aprovisionamiento de recursos es el proceso de 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 (VSANs), sistemas operativos invitados implementados en máquinas virtuales (VM) y enrutadores virtuales. Al igual que con los activos físicos, la implementación y retirada 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 funcionando después de una falla del equipo, corte de energía u otra interrupción. Implica el uso de componentes o instalaciones redundantes. La calidad de servicio (QoS) es una tecnología que administra los recursos de red para garantizar un nivel de servicio predefinido. Asigna prioridades de tráfico a los diferentes 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) son los siguientes:

- Ubicación geográfica
- Necesidades de la organización
- Costo de la ubicación
- Esfuerzo de restauración de la ubicación

16. a. La matriz redundante de discos independientes (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 pueden estar disponibles rápidamente desde los discos restantes de la matriz sin restaurar desde una cinta de copia de seguridad u otro medio de copia de seguridad. La agrupación en clústeres hace referencia a un producto de software que proporciona servicios de equilibrio de carga. Con la agrupación en clúster, una instancia de un servidor de aplicaciones actúa como controlador maestro y distribuye las solicitudes a varias instancias utilizando algoritmos round robin, weighted round robin o least-connections. 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 principal. 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 usan procesos complejos de reducción de números, como la utilización de cpu y memoria por servidor, los 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 de servidores.

17.c. Los registros de firewall registran información de tráfico de red, incluido el tráfico entrante y saliente. Esto suele incluir datos importantes, como direcciones IP y números de puerto que se pueden utilizar 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. Los registros de aplicaciones registran las acciones que se producen dentro de una aplicación específica. Los registros de cambios notifican los cambios realizados en un dispositivo o aplicación específicos como parte del proceso de administración de cambios.

18. d. La idea principal 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 de datos y el formato 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 las infracciones que superen ese umbral se registrarán para analizar por qué se produjeron las infracciones. Un control de dos personas, también conocido como una regla de dos personas, se produce 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 cercado a 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 solo disuaden a los intrusos ocasionales.
- Las vallas de 6 a 7 pies de altura son demasiado altas para escalar fácilmente.
- Las cercas de 8 pies y más altas disuaden a los intrusos más determinados, especialmente cuando se aumentan con alambre de afeitar.

Una geo-cerca es un área geográfica dentro de la cual los dispositivos se gestionan utilizando algún tipo de comunicación por radiofrecuencia. Se utiliza para realizar un seguimiento de 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 han reforzado en la medida de lo posible y aún así proporcionar funcionalidad. Se pueden realizar las siguientes acciones para reforzar lógicamente un sistema:

- Quitar aplicaciones innecesarias.
- Deshabilite los servicios innecesarios.
- Bloquear puertos no adquiridos.
- Controle firmemente la conexión de dispositivos de almacenamiento externos y medios si está permitido.