CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Plan de respuesta a incidentes

Responder eficazmente a los problemas de ciberseguridad

Establecer prácticas y políticas de preparación cibernética ayuda a reducir el riesgo, pero es importante asumir que es probable que nuestra empresa tenga que lidiar con un incidente de seguridad en algún momento que podría afectar a las operaciones comerciales. Tratar de determinar cómo responder en medio de un incidente no es una buena idea. El tiempo de respuesta es fundamental para minimizar el daño. Tener un plan claro puede marcar la diferencia entre un incidente y una catástrofe.

Visión general

Un plan de respuesta a incidentes completo, paso a paso, nos equipa para responder, resolver y aprender rápidamente de cada incidente. Este plan de respuesta a incidentes sirve como una hoja de ruta sobre qué hacer al responder a un incidente de seguridad, para garantizar que tengamos una respuesta estratégica en lugar de reactiva.

Hay tres elementos principales en nuestra respuesta a incidentes:

1. **Prepararse** para un posible incidente futuro
2. **Responder** durante el incidente
3. **Recuperarse** del incidente

Cómo prepararse

Pautas organizativas:
Como en tantas otras cosas, un poco de preparación es muy útil. Hay algunas acciones esenciales que deben realizarse lo antes posible para prepararse adecuadamente y reducir el daño de un ataque.

1. **Realice una copia de seguridad de los datos y asegúrese de que puede volver a instalar desde las copias de seguridad.** La recuperación de un ataque será mucho más rápida y afectará mucho menos a las operaciones si tiene copias de seguridad actuales del software de su sistema, las aplicaciones y especialmente de sus datos importantes. También querrá asegurarse de que cada persona de su organización tenga copias de seguridad si no lo hace de forma centralizada. Es importante probar periódicamente sus copias de seguridad.

    - ✓ Fecha de finalización: [FECHA]

2. **Asegúrese de que todos sepan cómo notificar un posible incidente.** La detección temprana es realmente importante. Cada miembro del equipo debe saber cómo detectar actividades sospechosas y a quién contactar al respecto.

    - ✓ Contacto designado para incidentes internos: [DETALLES DE CONTACTO]
    - ✓ Fecha de finalización: [FECHA]

3. **Encuentre un buen soporte técnico de respuesta a incidentes externos.** Sepa a quién acudir y cómo comunicarse con ellos en caso de emergencia. Un incendio que está más allá de su capacidad de control significa llamar a los bomberos. Necesita saber a quién llamar si un incidente cibernético está más allá de su capacidad de control. Como mínimo, debe ser un experto en soporte de TI que conozca y en el que confíe. Dependiendo del tamaño y la naturaleza de su negocio, es aconsejable identificar comunicaciones adicionales y soporte legal.

    - ✓ Contacto designado para incidentes externos: [DETALLES DE CONTACTO]
    - ✓ Fecha de finalización: [FECHA]

Cómo responder

Algo loco está sucediendo en el ordenador de un empleado y este no sabe qué hacer. Es el equivalente a oler humo o ver una pequeña llama en la sala de café.

Esto es lo que debe hacer:

1. **Aislar el problema:** desconecte inmediatamente el dispositivo de la red
2. **Identificar el tipo de incidente** y realizar la siguiente acción:
   - ✓ Malware: desconecte el dispositivo de la red inmediatamente
   - ✓ Robo de credenciales: deshabilite la cuenta, pero no la elimine, y restablezca la contraseña
   - ✓ Violación de datos: llame al contacto de emergencia de TI
   - ✓ Ransomware: desconecte el dispositivo de la red inmediatamente
   - ✓ Denegación de servicio: póngase en contacto con su responsable/TI/proveedor de servicios de Internet
3. **Determinar el alcance** del incidente haciendo estas preguntas:
   - ✓ ¿Cuándo ocurrió el incidente?
   - ✓ ¿Quién se ha visto afectado?
   - ✓ ¿Cuál es la naturaleza técnica del incidente? ¿Cómo ocurrió?
   - ✓ ¿Quién conoce el incidente?
   - ✓ ¿Sigue en curso?
4. **Determinar si se puede controlar adecuadamente internamente** o si necesita llamar a soporte de TI externo para asegurarse de que el ataque se gestione de manera adecuada.
5. **Seguir comprobando si el problema vuelve a ocurrir.** Si no está claro si el problema se ha resuelto, actúe con precaución y póngase en contacto con un experto sobre el problema.

Cómo recuperarse

La crisis terminó y ahora es el momento de que las cosas vuelvan a la normalidad. El alcance del incidente y la gravedad del impacto determinarán cuánto tiempo y esfuerzo se necesitará para recuperarse. Sin embargo, los pasos básicos son los mismos.

Esto es lo que debe hacer.

1. Notificar a todas las partes afectadas
2. Volver a definir la identificación de usuario y la contraseña del dispositivo atacado
3. Aplicar parches a todos los dispositivos
4. Reinstalar el software y los datos de las copias de seguridad según sea necesario

Lista de comprobación de respuesta a incidentes

Esta lista de comprobación es para ayudar al responsable de TI o líder en ciberseguridad

Prepararse

1. Copia de seguridad diaria
    - ✓ **Configuración de copia de seguridad automática/confirmada: [FECHA]**
2. Prueba de las copias de seguridad cada tres meses
    - ✓ **Fecha de última finalización: [FECHA]**
3. Protocolo IRP Comunicar a los trabajadores
    - ✓ **Fecha de última finalización: [FECHA]**

El contacto de emergencia de TI es: _____
El proveedor de servicios de Internet es: _____
El contacto de emergencia legal es: _____
El contacto de emergencia de comunicaciones es: _____

Responder

1. Aislar el problema: desconecte inmediatamente el dispositivo de la red
2. Identificar el tipo de incidente
    - ☐ Robo de credenciales
    - ☐ Ransomware
    - ☐ Malware
    - ☐ Denegación de servicio
    - ☐ Pérdida de datos confidenciales
3. Determinar el alcance del incidente
    - ☐ ¿A quién ha afectado?
    - ☐ ¿Cuándo empezó?
    - ☐ ¿Sigue sucediendo?

Recuperarse

1. Notificar a todas las partes
2. Volver a definir la identificación de usuario y la contraseña del dispositivo atacado
3. Aplicar parches a todos los dispositivos
4. Reinstalar el software y los datos de las copias de seguridad según sea necesario

Orientación adicional para la respuesta a incidentes

Esta guía sirve para ayudar al responsable de TI o al líder cibernético

Si desea tener un plan de respuesta a incidentes aún más sólido para su organización, a continuación se muestra un enfoque de cuatro pasos para hacerlo, basado las pautas del Instituto Nacional de Estándares y Tecnología (NIST). Puede que no sea completamente factible para usted seguir cada paso, pero haga todo lo posible para actuar en cada uno de los cuatro pasos de manera que tenga sentido para usted y su organización.

1 Preparación

La preparación es la clave para una respuesta rápida. En este paso debe elaborar una lista de todos sus activos, es decir, lo que hace que su empresa funcione. Esta lista incluirá, entre otras cosas, servidores, redes, aplicaciones y puntos de conexión críticos (como ordenadores portátiles). Una vez que haya compilado su lista de activos, clasifíquelos por nivel de importancia. Luego, supervise sus patrones de tráfico para poder crear líneas de base que se utilizarán para realizar comparaciones más adelante, o contrate a un proveedor para que supervise sus patrones de tráfico si sus recursos lo permiten. Si no puede permitirse un proveedor, una lista de activos y una atención priorizada hacia sus activos es un buen primer paso. Cree un plan de comunicaciones, con orientación sobre a quién contactar, cómo y cuándo en función de cada tipo de incidente. No olvide comunicarse con todas las personas de esta lista antes de que ocurra una crisis. Un refrán común en la gestión de crisis es "Nunca debe intercambiar tarjetas de presentación durante una crisis". Asegúrese de que todos en su lista sepan lo que espera de ellos durante una crisis.

Determine qué eventos de seguridad, y en qué umbrales, activarían su plan de respuesta a incidentes. Para ayudarle a identificar los umbrales, piense en lo que interrumpirá sus operaciones comerciales.

Después de identificar esos umbrales, cree un plan de respuesta a incidentes para cada tipo de incidente. Puede mejorarse a través de ejercicios de mesa, durante los cuales se identifican brechas en el proceso, pero también se mejorará después de los acontecimientos reales (más adelante se hablará de ello). La cuestión es que hay que establecer un proceso.

2 Detección y análisis

En este punto del proceso, se ha identificado un incidente de seguridad. Aquí es donde entra en modo de investigación. Recopile toda la información que pueda sobre el incidente. Luego analice los datos. Determine el punto de entrada y la amplitud de la brecha. Este proceso se hace sustancialmente más fácil y rápido si tiene todas sus herramientas de seguridad filtradas en una sola ubicación. Es posible que haya contratado a un proveedor que pueda realizar estas funciones por usted.

3 Contención, erradicación y recuperación

La contención tiene como objetivo detener el sangrado. Aquí es donde se aplicar el parche al punto de entrada de la amenaza.

La erradicación tiene como objetivo eliminar la amenaza. Si la amenaza entró desde un sistema y se propagó a otros sistemas, tendrá más trabajo.

La recuperación tiene como objetivo conseguir que el sistema esté operativo si se ha caído o simplemente volver a la normalidad si no lo ha hecho.

4 Lecciones aprendidas

Este paso brinda la oportunidad de aprender de su experiencia para que pueda responder mejor a futuros eventos de seguridad. Aunque sea tentador saltárselo, sobre todo con la interminable lista de tareas pendientes, este paso es muy recomendable.

Analice el incidente con una mirada humilde pero crítica para identificar las áreas de mejora. Luego añada esas mejoras a su documentación.

Ningún proceso es perfecto para todos los escenarios posibles. Algunos escenarios ni siquiera se pueden imaginar hasta que ocurren. El panorama de las amenazas también está en constante evolución, por lo que su proceso de respuesta a incidentes necesitará que se actualice de vez en cuando. Recuerde, su yo futuro se lo agradecerá. Como dice el refrán, "No desperdicies una buena crisis".