Conceptos básicos del Plan de respuesta a incidentes (IRP)

DESCRIPCIÓN GENERAL

Un Plan de respuesta a incidentes (IRP, por sus siglas en inglés) es un documento escrito, aprobado formalmente por el equipo de liderazgo superior, que ayuda a su organización *antes*, *durante* y *después* de un incidente de seguridad confirmado o sospechado. El IRP aclarará las funciones y responsabilidades, y brindará orientación sobre actividades clave. También debe incluir una lista de personas clave que pueden ser necesarias durante una crisis.

ANTES DE UN INCIDENTE DE CIBERSEGURIDAD

- **Capacite al personal**. Todo el personal debe comprender su papel en el mantenimiento y la mejora de la seguridad de la organización. Eso incluye saber cómo denunciar eventos sospechosos. Sea amable cuando la gente denuncie falsas alarmas. Recompense a las personas que se acerquen a denunciar eventos sospechosos como parte de su compromiso con una cultura de seguridad.
- **Revise su plan con un abogado**. Su abogado puede indicarle que utilice una plantilla completamente diferente para el IRP. Los abogados a menudo tienen preferencias sobre cómo interactuar con proveedores externos de respuesta a incidentes, las fuerzas del orden y otras partes interesadas.
- **Conozca a su equipo regional de la CISA**. Puede encontrar la información de su oficina regional aquí. Dentro de cada región de la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA, por sus siglas en inglés) se encuentran sus asesores de seguridad de protección (PSA, por sus siglas en inglés), asesores de seguridad cibernética (CSA, por sus siglas en inglés), coordinadores de la división de comunicaciones de emergencia y otro personal de la CISA locales y regionales para manejar una amplia gama de necesidades.
- **Conozca al equipo de su agencia local de seguridad pública (LEA, por sus siglas en inglés)**. Junto con su abogado, conozca a la policía local o a los representantes de la FBI. El momento de descubrir cómo notificar a los representantes de la agencia de seguridad pública (LEA) no es durante el fragor de la batalla.
- **Imprima estos documentos** y la lista de contactos asociada, y entregue una copia a todas las personas que espera que desempeñen un papel en un incidente. Durante un incidente, sus servicios internos de correo electrónico, chat y almacenamiento de documentos pueden estar inactivos o ser inaccesibles.
- **Desarrolle un plan de personal y partes interesadas para incidentes**. ¿Qué roles desempeñará cada uno? ¿A qué personas y grupos, que no serán lo más importante durante el incidente, habrá que notificar? Entre los ejemplos, se incluyen la junta directiva, los inversores clave y los socios críticos.
- **Revise este plan trimestralmente**. Los mejores IRP son documentos vivos que evolucionan con los cambios comerciales.
- **Prepare las respuestas de prensa con antelación**. Si un periodista lo llama y le dice que le han robado datos de sus servidores de archivos, ¿qué le dirá? Tener un buen "comunicado dilatorio" será útil.
- **Seleccione un recurso técnico o una empresa externo** que investigue posibles ataques.
- **Realice un ejercicio de simulación de ataque**, a veces denominado ejercicio teórico o TTX, por sus siglas en inglés. Un TTX es un juego de rol en el que un moderador presenta un escenario al equipo. El ejercicio podría comenzar cuando el jefe de comunicaciones recibe un correo electrónico de un periodista sobre rumores de un hackeo. El moderador brindará otras actualizaciones durante el juego para ver cómo cada uno desempeña su papel. Todo equipo deportivo practica, ¡y ustedes también deberían hacerlo!

DURANTE UN INCIDENTE DE CIBERSEGURIDAD

- **Asigne un gerente de incidentes (IM, por sus siglas en inglés).** Esta persona lidera la respuesta, gestiona los flujos de comunicación, actualiza a las partes interesadas y delega tareas. Sin embargo, el gerente de incidentes (IM) no realiza ninguna tarea técnica. Durante una época de crisis, la dilatación del tiempo afecta la percepción que las personas tienen de su paso. El IM controlará el reloj para evitar ese problema común. También puede dirigir la reunión retrospectiva (que se describe a continuación) para recopilar las lecciones aprendidas.

- **Asigne un gerente técnico (TM, por sus siglas en inglés).** El TM actuará como experto en la materia. Traerá a otros expertos técnicos internos y quizás externos (con el consentimiento del IM y posiblemente de su abogado).
- **Asigne un gerente de comunicaciones (CM, por sus siglas en inglés).** El CM interactuará con los periodistas, publicará actualizaciones en las redes sociales y podrá interactuar con partes interesadas externas (como accionistas).

DESPUÉS DE UN INCIDENTE DE CIBERSEGURIDAD

- **Celebre una reunión retrospectiva formal** (a veces denominada "post mortem"). En retrospectiva, el IM notificará el cronograma del incidente conocido y solicitará adiciones y ediciones. Luego, solicitará un análisis al equipo de respuesta a incidentes y sugerirá áreas de mejora.
    - **Nota: Las retrospectivas deben estar *libres de culpas***. Para que las retrospectivas tengan algún valor, cada uno de los participantes deben sentirse libres de discutir el incidente con libertad en un ambiente seguro y de apoyo. Los incidentes de seguridad rara vez son el resultado de la acción de una sola persona. Casi siempre son el resultado de una falla del *sistema* en general. La retrospectiva examinará *las personas, los procesos y las tecnologías*. La atención debe centrarse en los *procesos* y en las formas de mejorarlos.
- **Actualice las políticas y los procedimientos** de acuerdo a la reunión retrospectiva.
- **Comunique** los hallazgos a su personal. La transparencia genera confianza, y muchos empleados apreciarán saber que el equipo directivo se toma en serio la seguridad. Así es como se construye una cultura de seguridad.

VER TAMBIÉN

- Guía del Instituto Nacional de Estándares y Tecnología (NIST): https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- Orientación de la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA): https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal- government-cybersecurity-incident-and-vulnerability