

GUÍA DE RESPUESTA A INCIDENTES

PREPARACIÓN

- Trabaje con el equipo directivo sénior de su organización y con otro personal relevante para desarrollar un plan de respuesta a incidentes y continuidad del negocio basado en los riesgos más urgentes que se han identificado en la evaluación de riesgos cibernéticos de su organización.
 - Desarrolle escenarios de amenazas para los tipos de incidentes relacionados con los riesgos cibernéticos de mayor prioridad de su organización. Céntrese en el fomento de la capacidad para responder a esos escenarios.
 - Identifique, registre y ponga a disposición dentro de su organización una lista de puntos de contacto para la respuesta a incidentes.
 - Identifique y registre la información de contacto de las agencias y funcionarios de cumplimiento de la ley locales y federales pertinentes.
 - Establezca disposiciones que especifiquen qué tipos de incidentes deben notificarse, cuándo deben notificarse y a quién.
 - Establezca directrices escritas que describan la rapidez con la que el personal debe responder a un incidente y qué acciones deben realizarse, basándose en factores relevantes como el impacto funcional y de información del incidente, y la probable recuperación del incidente.
 - Informe a todos los empleados de que deben ponerse en contacto con su equipo técnico (con mayor frecuencia, será el personal de TI, el CISO/CIO u otro gerente comparable) cuando ocurra un incidente.
 - Implemente soluciones para supervisar las acciones de los empleados y permitir la identificación de amenazas e incidentes.
 - Incluya planes de continuidad del negocio para coordinar cómo funcionará su organización con los proveedores y los clientes principales durante una emergencia empresarial, que incluye cómo realizaría operaciones comerciales manuales o alternativas, si fuera necesario.
 - Incluya procedimientos escritos para apagar y reiniciar el sistema de emergencia.
 - Desarrolle y pruebe métodos para recuperar y restaurar datos de una copia de seguridad; compruebe periódicamente los datos de una copia de seguridad para verificar su validez.
 - Tenga establecidos acuerdos y procedimientos para llevar a cabo operaciones comerciales en instalaciones/centros alternativos.
 - Tenga un canal de difusión claro para todos los clientes.

EJERCICIOS

- Organice pequeños ejercicios de simulación con todo el personal o representantes de todos los niveles de personal, incluidos ejecutivos de la organización, personal de RR. PP./comunicaciones y equipos legales y de cumplimiento.
- Identifique, e idealmente participe, en ejercicios de simulación de todo el sector relevantes para su organización.
- Establezca el proceso para garantizar que las lecciones aprendidas de los ejercicios se incorporan y abordan en la estrategia de ciberseguridad de su empresa.

RESPUESTA

- Implemente acciones del plan de respuesta a incidentes para minimizar el impacto, incluido con respecto a daños a la reputación.
- Identifique los sistemas afectados/comprometidos y evalúe los daños.
- Reduzca los daños eliminando (desconectando) los activos afectados.
- Comience a registrar toda la información tan pronto como el equipo sospeche que se ha producido un incidente. Intente conservar pruebas del incidente al desconectar/segregar el activo identificado afectado, por ejemplo, recopilando los registros de configuración del sistema, red y detección de intrusión de los activos afectados.
- Notifique a las partes internas, proveedores externos y autoridades pertinentes, y solicite ayuda si es necesario.
- Inicie las actividades de notificación y asistencia al cliente de acuerdo con las leyes, las normativas y las directrices entre agencias.
- Utilice plataformas de intercambio de amenazas como FS-ISAC o MISP (Malware Information Sharing Platform [Plataforma de intercambio de información sobre malware]) para notificar a la industria sobre la amenaza.
- Documente todos los pasos que se llevaron a cabo durante el incidente para revisarlos más tarde.

RECUPERACIÓN

- Restaure los activos recuperados a "puntos de recuperación" periódicos si están disponibles y utilice datos de una copia de seguridad para restaurar los sistemas al último estado "bueno" conocido.
- Cree copias de seguridad "limpias" actualizadas de activos restaurados y garantice que todas las copias de seguridad de los activos críticos se almacenan en una ubicación protegida a nivel físico y medioambiental.
- Compruebe y verifique que los sistemas infectados estén completamente restaurados. Confirme que los sistemas afectados funcionan con normalidad.

REVISIÓN

- Lleve a cabo una conversación de “lecciones aprendidas” después de que se produzca el incidente: reúnanse con el personal sénior, asesores de confianza y proveedores de asistencia informática para revisar posibles vulnerabilidades o recomendar nuevos pasos a implementar.
- Si es posible, identifique las vulnerabilidades (ya sea en software, hardware, operaciones empresariales o comportamiento del personal) que causaron el incidente y desarrolle un plan para mitigarlos.
- Desarrolle un plan de supervisión para detectar incidentes similares o adicionales relacionados con los problemas identificados.
- Comparta lecciones aprendidas e información sobre el incidente en plataformas de intercambio de amenazas como FS-ISAC.
- Integre las lecciones aprendidas en los protocolos de respuesta a incidentes de su organización.

