Costo: $	Impacto: ALTO	Complejidad: BAJA

2.S: ¿Tiene el WWS un plan de respuesta a incidentes (IR) de ciberseguridad escrito para situaciones de amenazas críticas (p. ej., deshabilitación o manipulación de sistemas de control de procesos, pérdida o robo de datos operacionales o financieros, exposición de información sensible) que se implementa y actualiza de manera periódica?

Recomendación: Desarrolle, implemente y actualice un plan de IR para incidentes de ciberseguridad que puedan afectar las operaciones del WWS. Participe en ejercicios basados en el debate (p. ej., TTX) y basados en operaciones (p. ej., simulacros) para mejorar la respuesta a posibles incidentes informáticos.

¿Por qué es importante este control?

El plan de respuesta a incidentes de ciberseguridad es esencial para ayudar a su WWS a recuperarse rápidamente de incidentes de ciberseguridad. El plan de respuesta a incidentes describe las estrategias, los recursos y los procedimientos para prepararse y responder a un incidente informático. Puede incorporar el plan de respuesta a incidentes al plan de respuesta a emergencias (ERP) y usarlo como parte de la planificación de contingencias (consulte la hoja informativa 5.A).

Consejos de implementación

Identifique al personal, al personal de soporte de TO y TI y a los distribuidores que su WWS debe incluir en el desarrollo o la actualización del plan IR.

Desarrolle el plan IR de ciberseguridad para incluir lo siguiente:

- Funciones y responsabilidades definidos y acciones que todo el personal del WWS realizará durante y después de un incidente.
- Procedimientos para manejar el WWS en modo manual o procedimientos alternativos para mantener el servicio de agua si un ataque compromete el sistema de TO.
- Referencias a otros planes y procedimientos de respuesta relevantes según sea necesario.

ORIENTACIÓN ADICIONAL

- Un buen punto de partida para desarrollar un plan de respuesta a incidentes es la "Lista de verificación de medidas a incidentes de ciberseguridad" de la EPA. La realización de simulacros y ejercicios periódicos, como ejercicios prácticos, es esencial para una respuesta de emergencia eficaz a fin de minimizar los impactos adversos de un incidente informático. El WWS debe planificar y realizar ejercicios con la participación del personal del WWS, el personal de soporte de TO y TI, los distribuidores y los socios de respuestas a emergencias. Si los simulacros y ejercicios son nuevos para el WWS, utilice una situación que sea simple y realista. Por ejemplo, desarrolle una situación basada en un ataque de ransomware, ya que es un método de ataque común. La meta es ejercitar y evaluar los planes, políticas y procedimientos existentes y actualizarlos con las lecciones aprendidas. Realizar ejercicios también ayudará a desarrollar las capacidades de respuesta a los ataques informáticos del WWS. Después de realizar los ejercicios, el WWS debe realizar una sesión informativa sobre el ejercicio. La sesión informativa proporciona una oportunidad para que los participantes del ejercicio brinden comentarios sobre lo que sucedió durante el ejercicio y los obstáculos o desafíos que encontraron, y para identificar cualquier deficiencia en los planes, políticas y procedimientos del WWS que se deba abordar.

- Diagramas y otros elementos visuales para ayudar a todo el personal del WWS a comprender sus funciones, responsabilidades y acciones.
- Formularios de plantilla que el personal del WWS puede usar para registrar decisiones, acciones y gastos.
- Procedimientos e información de contacto para informar sobre el incidente (consulte la hoja informativa 4.A).

Distribuya el plan IR y capacite a todo el personal del WWS sobre los nuevos procedimientos o medidas de ciberseguridad en el plan IR mediante la realización de simulacros y ejercicios.

Revise el plan IR anualmente, como mínimo, y realice cambios según sea necesario, como cambios en el personal, los distribuidores y la información de contacto.

Actualice el plan de IR después de cualquier cambio significativo en los sistemas de TO y TI y en función de las lecciones aprendidas de un ejercicio o incidente real.

Recursos

Lista de verificación de medidas a incidentes de ciberseguridad de la EPA: Proporciona una lista de verificación práctica para ayudar a los WWS a prepararse, responder y recuperarse de incidentes informáticos. *https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf*

Los 12 fundamentos de ciberseguridad para sistemas de agua potable y aguas residuales de WaterISAC: Fundamento 1 (Plan para incidentes, emergencias y desastres) proporciona información y recursos para desarrollar un plan de respuesta a incidentes. *https://www.waterisac.org/fundamentals*

Guía de plantillas de gestión de políticas del NIST: Consulte la Política de respuesta a incidentes. Plantilla de política de respuesta a incidentes que las empresas de servicios públicos pueden utilizar para desarrollar una política de respuesta a incidentes. *https://www.cisecurity.org/wp-content/uploads/2020/06/Incident-Response-Policy.docx*

Herramientas de respuesta a incidentes informáticos de la CISA: Proporciona capacitación y manuales sobre respuesta a incidentes. *https://www.cisa.gov/cyber-incident-response*

Herramienta de ejercicios prácticos de la EPA: Proporciona a los usuarios recursos para planificar, realizar y evaluar ejercicios prácticos. *https://ttx.epa.gov/*

Paquetes de ejercicios prácticos de la CISA (CTEP): Proporciona herramientas para que las partes interesadas realicen ejercicios de planificación en una amplia gama de situaciones de amenazas. Los socios pueden utilizar los CTEP para iniciar debates dentro de sus organizaciones sobre su capacidad para abordar una variedad de situaciones de amenazas. Proporciona a los usuarios recursos para planificar, realizar y evaluar ejercicios prácticos. *https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages*

Principales medidas informáticas para proteger los sistemas de agua de la CISA: Consulte el punto 5 de la página 2 de este recurso para obtener información adicional. *https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*