Costo: $$	Impacto: ALTO	Complejidad: MEDIO

2.R: ¿Realiza el WWS copias de seguridad de los sistemas necesarios para las operaciones (p. ej., configuraciones de red, lógica de PLC, diagramas de ingeniería, registros de personal) según un cronograma periódico, almacena las copias de seguridad separadas de los sistemas de origen y prueba las copias de seguridad de manera periódica?

Recomendación: Realice copias de seguridad periódicas de los sistemas de TO/TI para que pueda recuperarlos a un estado conocido y seguro en el caso de que se vean comprometidos. Pruebe los procedimientos de copia de seguridad y aísle las copias de seguridad de las conexiones de red. Implemente la regla 3-2-1 del NIST:

3) Conserve tres copias: una primaria y dos de seguridad.

2) Conserve las copias de seguridad en dos tipos de medios diferentes.

1) Almacene una copia fuera del sitio.

¿Por qué es importante este control?

Las copias de seguridad son un elemento fundamental de las actividades de restauración y recuperación de su WWS en caso de un incidente informático, un mal funcionamiento del *hardware* (p. ej., una falla del disco duro) o la destrucción física del equipo (p. ej., un incendio, una inundación). Las copias de seguridad son una de las primeras líneas de defensa más importantes para evitar tener que pagar rescates y restaurar rápidamente las operaciones.

Consejos de implementación

Identificar todos los datos operacionales, de clientes, de empleados, financieros y de otro tipo que su empresa de servicios públicos pueda perder o que un atacante pueda corromper durante un incidente es crucial para restaurar las operaciones normales después del incidente. Realizar copias de seguridad periódicas de los sistemas de TO/TI garantiza que pueda recuperar un estado conocido y seguro en caso de que se vean comprometidos. Implementar la regla 3-2-1 del NIST es esencial: mantenga tres copias de sus datos (una principal y dos de seguridad), almacene las copias de seguridad en dos tipos de medios

ORIENTACIÓN ADICIONAL

- El WWS debe realizar copias de seguridad utilizando el enfoque de "copia de seguridad en profundidad", con capas de copias de seguridad (p. ej., local, en las instalaciones, para desastres) que estén secuenciadas en el tiempo de modo que las copias de seguridad locales recientes estén disponibles para su uso inmediato y las copias de seguridad seguras estén disponibles para recuperarse de un gran incidente de ciberseguridad. El enfoque de "copias de seguridad en profundidad" se basa en que una empresa de servicios públicos tenga tres copias de sus datos, utilice al menos dos medios de almacenamiento diferentes y almacene al menos una copia de forma remota fuera del sitio o en la nube. El WWS debe utilizar múltiples enfoques de copias de seguridad/restauración y métodos de almacenamiento para garantizar que las copias de seguridad se generen rigurosamente, se almacenen de forma segura y sean accesibles de forma adecuada para su restauración.

diferentes y guarde una copia fuera del sitio para protegerse contra incidentes locales como incendios o inundaciones.

Proteja los medios de las copias de seguridad almacenándolos por separado de los sistemas de los que se hacen las copias siempre que sea posible, utilizando copias de seguridad externas basadas en la nube o rotaciones de copias de seguridad manuales, como intercambiar varias unidades de copias de seguridad periódicamente con una siempre almacenada fuera del sitio.

Establezca un procedimiento para garantizar que el proceso de copia de seguridad se siga según un cronograma específico y que las copias de seguridad de los archivos se puedan usar. Pruebe periódicamente las copias de seguridad para confirmar que sean efectivas, verificando al azar el tamaño de un archivo y la fecha de modificación de los archivos de las copias de seguridad en los medios de recuperación y validando la capacidad de recuperar archivos individualmente.

En el caso de los activos de TO, asegúrese de que las copias de seguridad incluyan elementos como la lógica del PLC y los gráficos de HMI para permitir una rápida restauración de estos componentes críticos.

Como mínimo, realice copias de seguridad y pruebe los sistemas de TO y TI anualmente para garantizar la confiabilidad y la eficacia de sus procedimientos de copia de seguridad y recuperación.

Recursos

Estándar 800-82 (revisión 3) del NIST, Guía para la seguridad de la tecnología operacional (TO): Puede encontrar información adicional sobre las copias de seguridad en la sección 6.2.4.3 (página 112).
https://csrc.nist.gov/pubs/sp/800/82/r3/final

Estándar 800-34 del NIST, Guía de planificación de contingencias para sistemas de información federales: Puede encontrar información adicional sobre los procedimientos generales y las buenas prácticas para realizar copias de seguridad en la sección 3.4.2 (página 21).
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Principales medidas informáticas para proteger los sistemas de agua de la CISA: Consulte el punto 6 de la página 2 de este recurso para obtener información adicional.
https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems