Costo: $	Impacto: ALTO	Complejidad: BAJA

2.J: ¿Ofrece el WWS capacitación sobre ciberseguridad específica de TO al menos anualmente al personal que usa TO como parte de sus tareas habituales??

Recomendación: Proporcione capacitación especializada sobre ciberseguridad enfocada en TO a todo el personal que utilice activos de TO.

¿Por qué es importante este control?

La importancia de una capacitación periódica sobre ciberseguridad para todo el personal se aborda en la hoja informativa 2.I. Además, el personal que mantiene o protege TO como parte de sus tareas habituales debe recibir capacitación sobre ciberseguridad específica de TO al menos anualmente.

Consejos de implementación

Identifique al personal del WWS que debe recibir una capacitación más especializada en ciberseguridad centrada en TO. Como mínimo, los WWS deben proporcionar esta capacitación especializada al personal que usa activos de TO como parte de sus tareas habituales.

Recursos

Capacitación sobre ICS de la CISA: Proporciona capacitación en línea sin costo sobre una variedad de temas de seguridad de TO. *https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA*

Guía de plantillas de políticas del NIST: Consulte la Política de capacitación y concientización sobre seguridad. Cronogramas de capacitación, registros, presentaciones, etc. que demuestran que esta capacitación específica de TO se lleva a cabo al menos una vez al año. *https://www.cisecurity.org/wp-content/uploads/2020/06/Security-Awareness-and-Training-Policy.docx*

Estándar 800-82 (revisión 3) del NIST, Guía para la seguridad de la tecnología operacional (TO): La sección 6.2.2 en la página 108 proporciona orientación para capacitación sobre TO. *https://csrc.nist.gov/pubs/sp/800/82/r3/final*

ORIENTACIÓN ADICIONAL

- ✓ El distribuidor de TO designado del WWS puede ser capaz de realizar una capacitación sobre ciberseguridad centrada en TO para el WWS.
- ✓ En lugar de una gran capacitación que cubra muchos temas, un WWS debe realizar múltiples capacitaciones programadas periódicamente durante el año para ayudar a dividir los temas en sesiones breves y fáciles de digerir.
- ✓ Desarrolle la agenda y los materiales de capacitación para que sean fáciles de seguir y consultar más adelante. La capacitación debe cubrir la seguridad de los activos de TO, las configuraciones, las funciones de seguridad, las medidas de respuesta a incidentes y las operaciones generales. Si el WWS puede funcionar manualmente sin el uso de TO, considere agregar capacitación para operaciones manuales. Las operaciones manuales pueden ser una línea de defensa esencial para mantener el WWS operativo en caso de un ataque informático. Hay muchas oportunidades de capacitación disponibles en línea para el personal de los WWS, incluyendo las de la CISA y la NICCS (consulte los recursos).

NICCS Aprendizaje CISA: Proporciona capacitación gratuita en línea sobre ciberseguridad para empleados de gobiernos estatales, locales, tribales y territoriales.
https://niccs.cisa.gov/education-training/cisa-learning

Capacitación práctica de primer nivel sobre los ICS (SANS Institute): Esta capacitación pagada ofrece varios cursos diseñados para aumentar las habilidades de ciberseguridad de quienes usan TO/ICS en sus WWS.
https://www.sans.org/cyber-security-courses/?focus-area=industrial-control-systems-security&msc=main-nav