TLP:CLEAR

Principales acciones cibernéticas para proteger los sistemas hídricos

Descripción general

Las entidades del Sector de Sistemas de Agua y Aguas Residuales (en lo sucesivo denominados "sistemas hídricos") ejecutan sistemas de tecnología operativa (OT, por sus siglas en inglés) y de tecnologías de la información (IT, por sus siglas en inglés) que, con demasiada frecuencia, son vulnerables a los ataques cibernéticos. Esta hoja informativa destaca las principales medidas cibernéticas que los sistemas de abastecimiento de agua pueden tomar hoy para reducir el riesgo cibernético y mejorar la resistencia a los ciberataques, y proporciona servicios, recursos y herramientas gratuitos para apoyar estas medidas, que pueden tomarse simultáneamente.[1, 2,3] Visite las páginas web de la Agencia de Seguridad Cibernética y de Infraestructura (CISA, por sus siglas en inglés) sobre ciberseguridad de los sistemas de abastecimiento de agua y aguas residuales y de la Agencia de Protección del Medio Ambiente (EPA, por sus siglas en inglés) sobre ciberseguridad en el sector del agua para obtener más información y recursos.

Comprador, tenga cuidado: los fabricantes de tecnología toman decisiones de seguridad que afectan la calidad de su software y hardware. Revise la guía de Seguridad desde el diseño de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) y pregunte a sus proveedores cómo están implementando los principios y las tácticas de seguridad desde el diseño en sus productos para mitigar las amenazas a la ciberseguridad.

1. Reducir la exposición a la Internet pública

Utilice servicios de higiene cibernética para reducir la exposición de activos clave a la Internet pública. Los dispositivos OT, como controladores y unidades terminales remotas (RTU, por sus siglas en inglés), son objetivos fáciles para los ciberataques cuando están conectados a Internet.

- **Recurso gratuito:** en la hoja informativa sobre escaneo gratuito de vulnerabilidades cibernéticas para servicios públicos de agua de la Agencia de Seguridad Cibernética y de Infraestructura (CISA), se explica el proceso y los beneficios de registrarse en el programa gratuito de escaneo de vulnerabilidades de la CISA.
- **Servicio gratuito:** envíe un correo electrónico a vulnerability@cisa.dhs.gov con el asunto "Requesting Cyber Hygiene Services" (Solicitud de servicios de higiene cibernética) para obtener los servicios de higiene cibernética de la Agencia de Seguridad Cibernética y de Infraestructura (CISA), que identifican de forma proactiva y permiten la mitigación oportuna de activos expuestos a Internet.

2. Realizar evaluaciones periódicas de ciberseguridad

Realice una evaluación de ciberseguridad de forma periódica para comprender las vulnerabilidades existentes en los sistemas de OT y de IT. Las evaluaciones le permiten identificar, evaluar y priorizar la mitigación de vulnerabilidades en redes de OT y de IT.

- **Servicio gratuito:** las Evaluaciones de ciberseguridad de la Agencia de Protección del Medio Ambiente (EPA) pueden ayudar a evaluar la situación en cuanto a la ciberseguridad.
- **Recursos gratuitos:**
  - Los Objetivos de Desempeño de Ciberseguridad (CPG, por sus siglas en inglés) de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) proporcionan un conjunto de protecciones cibernéticas básicas. Puede realizar una evaluación gratuita de los Objetivos de Desempeño de Ciberseguridad (CPG) administrada por un asesor de ciberseguridad de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) (regiones de la CISA) o mediante una autoevaluación.

[1] La Agencia de Seguridad Cibernética y de Infraestructura (CISA, por sus siglas en inglés), la Agencia de Protección del Medio Ambiente (EPA, por sus siglas en inglés) y la Oficina Federal de Investigación (FBI, por sus siglas en inglés) han elaborado en conjunto esta hoja informativa.
[2] Aviso conjunto de FBI-CISA-NSA-EPA-INCD: Agentes cibernéticos afiliados al IRGC explotan PLC en varios sectores, incluidas instalaciones de WWS en los EE. UU.
[3] Aviso conjunto de ciberseguridad de FBI-CISA-EPA-NSA: Amenazas cibernéticas continuas a los sistemas de agua y aguas residuales de los EE. UU.

- La Guía de manejo de riesgos de ciberseguridad del sector hídrico y la Herramienta de manejo de riesgos de la Asociación Estadounidense de Obras Hidráulicas (AWWA, por sus siglas en inglés) pueden ayudar a una empresa de servicios públicos a examinar qué controles y prácticas de ciberseguridad son más pertinentes en función de las aplicaciones tecnológicas que implementaron.
- La Guía de manejo de riesgos de ciberseguridad del sector hídrico para sistemas pequeños de la Asociación Estadounidense de Obras Hidráulicas (AWWA) es una *guía de introducción*que ayuda a las pequeñas empresas de servicios públicos rurales (aquellas que prestan servicios a menos de 10,000 personas) a evaluar e implementar prácticas recomendadas cibernéticas.
- Los Quince principios básicos de ciberseguridad para servicios de agua y aguas residuales de WaterISAC proporcionan una descripción general de las medidas de ciberseguridad y recursos complementarios junto a cada medida para obtener más información.
- El Método de Evaluación de Riesgos del Center for Internet Security (CIS RAM, por sus siglas en inglés) de MS-ISAC es un método de evaluación de riesgos de seguridad de la información que ayuda a las organizaciones a implementar y evaluar su situación de seguridad frente a las prácticas recomendadas de ciberseguridad de los Controles de Seguridad Críticos del Center for Internet Security (CIS). En la colección de documentos del Método de Evaluación de Riesgos del Center for Internet Security (CIS RAM), se proporcionan instrucciones, ejemplos, plantillas y ejercicios para realizar una evaluación de riesgos cibernéticos.

3. Cambiar las contraseñas predeterminadas de inmediato

Exija contraseñas únicas, seguras y complejas para todos los sistemas hídricos, incluida la infraestructura conectada. Las contraseñas predeterminadas débiles o inseguras son fáciles de descubrir y explotar y pueden permitir que los actores de amenazas cibernéticas realicen cambios en los procesos operativos de los sistemas hídricos. Esto puede afectar de forma negativa la salud y la seguridad públicas. Cambie las contraseñas predeterminadas o inseguras e implemente la autenticación multifactor (MFA, por sus siglas en inglés) cuando sea posible. Concéntrese en implementar la MFA en la infraestructura de IT, como el correo electrónico, para dificultar que los agentes de amenazas accedan a los sistemas OT. Considere pedir a los fabricantes que eliminen las contraseñas predeterminadas.

- **Recursos gratuitos:** Campaña "Secure our World: Use Strong Passwords" de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) y campaña "More than a Password". Para obtener orientación cibernética adicional, consulte la Guía cibernética para pequeñas empresas de la CISA.

4. Realizar un inventario de activos de OT y de IT

Cree un inventario de activos de software y hardware para ayudar a comprender lo que necesita proteger. Centre los esfuerzos iniciales en dispositivos conectados a Internet y dispositivos donde las operaciones manuales no son posibles. Utilice la monitorización para identificar los dispositivos que se comunican en su red.

- **Servicio gratuito:** El Programa de Asistencia Técnica en Ciberseguridad de la Agencia de Protección del Medio Ambiente (EPA) le brinda ayuda para la realización de un inventario.
- **Herramienta gratuita:** un primer paso para realizar un inventario es identificar los dispositivos de la red. La herramienta Malcolm de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) permite la monitorización de la red con analizadores personalizados diseñados para protocolos de sistema de control industrial (ICS, por sus siglas en inglés) y de OT.

5. Desarrollar y ejecutar planes de respuesta y recuperación ante incidentes de ciberseguridad

Desarrollar

Comprenda las acciones de respuesta a incidentes, las funciones y las responsabilidades, así como a quién contactar y cómo informar un incidente cibernético antes de que ocurra para garantizar la preparación contra posibles ataques.

- **Recursos gratuitos:** La Lista de cotejo de acciones de ciberseguridad de la Agencia de Protección del Medio Ambiente (EPA) y los Conceptos básicos del Plan de Respuesta a Incidentes (IRP, por sus siglas en inglés) de la Agencia de Seguridad Cibernética e Infraestructura (CISA) ayudan a desarrollar planes de respuesta a incidentes cibernéticos. En la Guía conjunta de respuesta a incidentes relacionados con el agua de la Agencia de Seguridad Cibernética y de Infraestructura (CISA), la Oficina Federal de Investigaciones (FBI) y la Agencia de Protección del Medio Ambiente (EPA), se proporciona información valiosa sobre cómo trabajar con los colaboradores de respuesta federales antes, durante y después de un incidente cibernético. **Nota:** Consulte esta guía para obtener información de contacto de la Agencia de Seguridad Cibernética y de Infraestructura (CISA), la Oficina Federal de Investigaciones (FBI) y la División de Infraestructura del Agua y Resiliencia Cibernética de la Agencia de Protección del Medio Ambiente (EPA).

Ejecutar

Pruebe su plan de respuesta a incidentes anualmente para asegurarse de que todos los operadores estén familiarizados con sus funciones y responsabilidades.

- **Herramientas gratuitas:** las herramientas de escenarios del Paquete de ejercicios teóricos de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) (CTEP, por sus siglas en inglés) y del ejercicio teórico (TTX, por sus siglas en inglés) de la Agencia de Protección del Medio Ambiente (EPA) ayudan a los propietarios y operadores de infraestructuras críticas a desarrollar sus propios ejercicios teóricos para satisfacer sus necesidades específicas.

6. Realizar copias de seguridad de sistemas de OT y de IT

Realice copias de seguridad de los sistemas de OT y de IT de forma periódica para que pueda recuperarlos a un estado conocido y seguro en caso de peligro. Pruebe los procedimientos de respaldo y aísle las copias de seguridad de las conexiones de red. Implemente la regla 3-2-1 del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) que consiste en lo siguiente: 3) mantenga tres copias, una principal y dos de respaldo; 2) mantenga las copias de seguridad en dos tipos de medios diferentes; 1) guarde una copia fuera del sitio.

- **Recursos gratuitos:** Capítulo 5 del Kit de herramientas Cyber Essentials de la CISA: Sus datos y la Protección de datos contra ransomware y otros eventos de pérdida de datos del Instituto Nacional de Estándares y Tecnología (NIST) brindan orientación sobre cómo realizar copias de seguridad de los sistemas.

7. Reducir la exposición a las vulnerabilidades

Mitigue las vulnerabilidades conocidas y mantenga todos los sistemas actualizados con parches y actualizaciones de seguridad. Priorice los parches de OT de acuerdo con el catálogo de Vulnerabilidades explotadas conocidas (KEV, por sus siglas en inglés) de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) durante el periodo de inactividad programado de los equipos de OT; priorice los parches en IT, según corresponda. La campaña Secure our World de la CISA proporciona orientación sobre la actualización de software.

8. Impartir capacitación sobre concienciación en materia de ciberseguridad

Realice capacitación de concienciación sobre ciberseguridad de forma anual, como mínimo, para ayudar a todos los empleados a comprender la importancia de la ciberseguridad y cómo prevenir y responder a los ciberataques.

- **Recursos gratuitos:** consulte la Capacitación en ciberseguridad de la Agencia de Protección del Medio Ambiente (EPA) y la capacitación virtual gratuita en ciberseguridad de Sistemas de control industrial de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) para obtener información sobre la protección contra ataques cibernéticos a la infraestructura crítica. Consulte también la Campaña Secure our World de la Agencia de Seguridad Cibernética y de Infraestructura (CISA): capacitación sobre phishing para empleados a fin de conocer pasos prácticos para ayudar a sus empleados a evitar estafas de phishing.

Apoyo

Si necesita apoyo adicional para implementar cualquiera de estas acciones, comuníquese con la Agencia de Protección del Medio Ambiente (EPA) o con su asesor regional de ciberseguridad de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) para obtener asistencia.

Descargo de responsabilidad

Las agencias autoras no respaldan ninguna entidad comercial, producto, empresa o servicio, incluidas las entidades, los productos o los servicios vinculados o mencionados en este documento. Cualquier referencia a entidades comerciales, productos, procesos o servicios específicos mediante marcas de servicio, marcas comerciales, fabricantes o de otro modo, no constituye ni implica respaldo, recomendación ni favoritismo por parte de las agencias autoras.