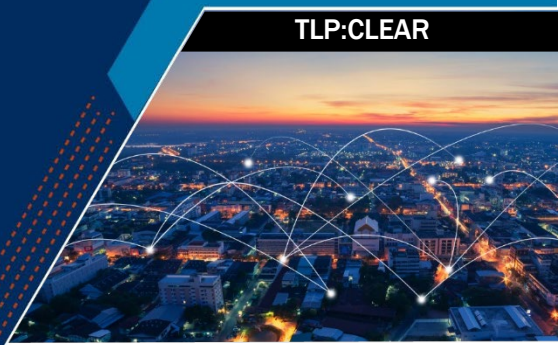
TLP:CLEAR

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 (operational technology, OT) y de tecnología informática (information technology, IT) que, con demasiada frecuencia, son vulnerables a los ataques cibernéticos. Esta hoja informativa destaca las principales acciones cibernéticas que los sistemas hídricos pueden tomar hoy para reducir el riesgo cibernético y mejorar la resiliencia a los ataques cibernéticos y proporciona servicios, recursos y herramientas gratuitos para apoyar estas acciones, que se pueden tomar al mismo tiempo.[1], [2], [3] Visite las páginas web de Ciberseguridad de los sistemas de agua y aguas residuales de la CISA y Ciberseguridad para el sector hídrico de la EPA 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 por diseño de la CISA y pregunte a sus proveedores cómo están adoptando los principios y tácticas de seguridad por diseño dentro de 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 de tecnología operativa como controladores y unidades terminales remotas (remote terminal units, RTU), 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 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 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 establecidas en los sistemas de OT e IT. Las evaluaciones le permiten identificar, evaluar y priorizar la mitigación de vulnerabilidades en redes de OT e IT.

- **Servicio gratuito:** las evaluaciones de ciberseguridad de la EPA pueden ayudar a evaluar la postura de ciberseguridad.
- **Recursos gratuitos:**
  - Las Metas de desempeño de ciberseguridad (Cybersecurity Performance Goals, CPG) de la CISA proporcionan un conjunto de protecciones cibernéticas básicas. Un asesor de ciberseguridad de la CISA (regiones de la CISA) puede realizar una evaluación de CPG gratuita o también puede realizarse mediante una autoevaluación.
  - La Guía de manejo de riesgos de ciberseguridad del sector hídrico y la Herramienta de manejo de riesgos de la American Water Works Association (AWWA) pueden ayudar a una empresa de servicios públicos a examinar qué controles y prácticas de ciberseguridad son más aplicables en función de las aplicaciones tecnológicas que han implementado.
  - La Guía de manejo de riesgos de ciberseguridad del sector hídrico para sistemas pequeños de la 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 mejores prácticas cibernéticas.
  - Los 15 fundamentos de ciberseguridad para servicios de agua y aguas residuales de WaterISAC proporcionan una descripción general de las medidas de ciberseguridad con recursos para acompañar cada medida para una exploración más profunda.
  - El Método de Evaluación de Riesgos del Center for Internet Security (CIS RAM) 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 postura de seguridad frente a las mejores prácticas de ciberseguridad de los Controles de Seguridad Críticos del CIS (CIS Controls). En la familia de documentos del CIS RAM se proporcionan instrucciones, ejemplos, plantillas y ejercicios para realizar una evaluación de riesgos cibernéticos.

[1] La Cybersecurity and Infrastructure Security Agency (CISA), la Environmental Protection Agency (EPA) y la Federal Bureau of Investigation (FBI) escribieron conjuntamente esta hoja informativa.
[2] Aviso conjunto FBI-CISA-NSA-EPA-INCD: Actores cibernéticos afiliados al IRGC explotan los controladores lógicos programables (Programmable Logic Controller, PLC) en múltiples sectores, incluidas las instalaciones del WWS de EE. UU.
[3] Aviso conjunto sobre ciberseguridad del FBI, la CISA, la EPA y la NSA: Amenazas cibernéticas continuas a los sistemas de agua y aguas residuales de EE. UU.

3. Cambie 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 (multifactor authentication, MFA) cuando sea posible. Concéntrese en implementar la MFA en la infraestructura de IT, como el correo electrónico, para dificultar que los actores de amenazas accedan a los sistemas de OT. Considere pedir a los fabricantes que eliminen las contraseñas predeterminadas.

- **Recursos gratuitos:** Campaña Secure our World de la CISA: utilice contraseñas seguras 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 OT/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 Cybersecurity Technical Assistance Program de la EPA lo apoya en la realización de un inventario.
- **Herramienta gratuita:** un primer paso para realizar un inventario es identificar los dispositivos en la red. La herramienta Malcolm de la CISA permite la monitorización de la red con analizadores personalizados diseñados para protocolos de sistema de control industrial (ICS)/OT.

5. Desarrollar y ejecutar planes de respuesta y recuperación de 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 EPA y los Fundamentos del Plan de Respuesta a Incidentes (Incident Response Plan, IRP) de la CISA ayudan a desarrollar planes de respuesta a incidentes cibernéticos. La Guía conjunta de respuesta a incidentes relacionados con el agua de la CISA, el FBI y la EPA 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 CISA, el FBI y la Water Infrastructure and Cyber Resilience Division de la 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 CISA (CTEP) y del ejercicio teórico (TTX) de la EPA ayudan a los propietarios y operadores de infraestructuras críticas a desarrollar sus propios ejercicios teóricos para satisfacer sus necesidades específicas.

6. Copias de seguridad de sistemas OT/IT

Realice copias de seguridad de los sistemas OT/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 NIST 3-2-1: 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:** el 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 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 (Known Exploited Vulnerabilities, KEV) de la 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 EPA y la capacitación virtual gratuita en ciberseguridad de Sistemas de control industrial de la CISA para aprender cómo protegerse contra ataques cibernéticos a la infraestructura crítica. Consulte también la campaña Secure our World de la CISA : capacitación sobre phishing para empleados para 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 EPA o con su asesor regional de ciberseguridad de la 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 específicas o productos, procesos o servicios mediante marcas de servicio, marcas comerciales, fabricantes o de otro modo no constituye ni implica respaldo, recomendación o favoritismo por parte de las agencias autoras.