Evaluación de la seguridad cibernética durante las inspecciones sanitarias del sistema público de agua

Oficina del Agua de la EPA (4608T)
EPA 817-B-23-001
Marzo de 2023

Descargo de responsabilidad

La División de Infraestructura del Agua y Resiliencia Cibernética de la Oficina de Agua Subterránea y Agua Potable revisó y aprobó este documento para su publicación. Este documento no impone requisitos legalmente vinculantes a ninguna de las partes. Ni el Gobierno de Estados Unidos ni ninguno de sus empleados o contratistas otorgan ninguna garantía, expresa o implícita, ni asumen ninguna obligación o responsabilidad legal por el uso por parte de terceros de cualquier información, producto o proceso mencionado en este documento, ni representan que su uso por dicha parte no infrinja los derechos de propiedad privada. La mención de nombres o productos comerciales no constituye respaldo o recomendación para su uso.

Comentario público

La Agencia de Protección Ambiental (EPA) de Estados Unidos invita al público a comentar sobre las secciones 4 a 8 y todos los apéndices de este documento de lineamientos. La EPA planea revisar y actualizar este documento según sea necesario en función de los comentarios públicos y la nueva información. Los comentarios sobre este documento deben dirigirse a wicrd-outreach@epa.gov.

Tabla de contenido

Apéndices

1.0 Antecedentes

1.1. ¿Cuál es el propósito de esta guía?

Esta guía respalda la implementación del memorándum de la Agencia de Protección Ambiental de EE. UU., *Abordar la seguridad cibernética del sistema público de agua (PWS) en las inspecciones sanitarias o en procesos alternativos*.[1] Los pasos descritos en el memorándum promueven la misión de la EPA de trabajar con los estados[2] para proteger el agua potable limpia y segura. El memorándum aclara que los estados deben evaluar la seguridad cibernética de la tecnología operativa[3] utilizada por el sistema público de agua al realizar una inspección sanitaria del PWS o por medio de otros programas estatales.

En el memorándum y en esta guía, se explican varios enfoques para incluir la seguridad cibernética en las inspecciones sanitarias del PWS o en otros programas estatales. El objetivo de las inspecciones sanitarias es garantizar que los estados identifiquen de manera eficaz las deficiencias significativas y que los PWS luego las corrijan —entre estas, se incluyen las relacionadas con la seguridad cibernética— que podrían afectar el agua potable segura. La EPA ofrece asistencia técnica significativa y apoyo a los estados en esta tarea, así como a los PWS para cerrar las brechas de la seguridad cibernética.

Hoy en día, los PWS son objetivos frecuentes de actividad cibernética maliciosa,[4] que tiene el mismo potencial o incluso mayor de comprometer el tratamiento y la distribución de agua potable segura que un ataque físico. Aclarar que la seguridad cibernética debe evaluarse durante las inspecciones sanitarias u otros programas estatales al revisar la tecnología operativa que forma parte del equipo o la operación de un PWS ayudará a reducir las probabilidades de un ataque cibernético exitoso en un PWS y mejorará la recuperación si se produce un incidente cibernético.

1.2. ¿Quién debería usar esta guía?

En esta guía, encontrará información extraída del memorándum y material complementario opcional para ayudar a los estados y a los PWS a abordar la seguridad cibernética de la tecnología operativa en las inspecciones sanitarias del PWS. Para obtener información general sobre las inspecciones sanitarias del PWS, incluida la legislación subyacente, los componentes y la frecuencia de las inspecciones y los materiales de referencia, consulte https://www.epa.gov/dwreginfo/sanitary-surveys.

---

[1] https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector

[2] "Estado" o "estados" globalmente en este documento incluye las tribus, los territorios y las regiones de la EPA donde tiene la autoridad de aplicación principal para los sistemas públicos de agua.

[3] El término "tecnología operativa" significa hardware y software que detecta o provoca un cambio a través del monitoreo o control directo de dispositivos físicos, procesos y eventos en la empresa. Ley de Mejora de la Ciberseguridad de Internet de las Cosas de 2020, 15 U.S.C., § 271 (3)(6) (Ley pública 116-207).

[4] Alerta (AA21-287A), Ongoing Cyber Threats to U.S. Water and Wastewater Systems (Amenazas cibernéticas continuas a los sistemas de agua y aguas residuales de EE. UU.),https://www.cisa.gov/uscert/ncas/alerts/aa21-287a

La EPA pretende que esta guía ayude tanto a los estados como a los PWS. Específicamente, el personal del estado involucrado en la planificación, la realización o la revisión de las inspecciones sanitarias del PWS puede usar esta guía para aprender lo siguiente:

- enfoques para evaluar la seguridad cibernética en los PWS a fin de cumplir con los requisitos de la inspección sanitaria, incluidos los recursos que pueden ayudar a los estados con la evaluación de la seguridad cibernética;
- cómo identificar las brechas en la seguridad cibernética de los PWS, incluidas las posibles deficiencias significativas; y
- acciones que los PWS pueden tomar para abordar las brechas de la seguridad cibernética, incluidas las deficiencias significativas si el estado las identifica.

Los PWS pueden usar esta guía para aprender lo siguiente:

- cómo evaluar las prácticas y los controles de seguridad cibernética actuales del PWS para identificar las brechas;
- acciones de desarrollo de un plan de mitigación de riesgos de seguridad cibernética del PWS para las brechas de seguridad cibernética, incluidas las deficiencias significativas si el estado las identifica; y
- recursos que pueden ayudar a cerrar las brechas de seguridad cibernética.

Nota: El memorándum y esta guía de apoyo se centran en la evaluación y la mejora de la seguridad cibernética de la tecnología operativa en los PWS a través de inspecciones sanitarias o programas alternativos del estado. No abarca todos los componentes necesarios para un programa integral de seguridad cibernética de infraestructura crítica, como los roles potenciales del estado en la notificación de incidentes cibernéticos y la respuesta ante ellos.

2.0 ¿Cuál es el requisito para evaluar la seguridad cibernética durante las inspecciones sanitarias del PWS?

La definición de una inspección sanitaria es "una revisión en el sitio de la fuente de agua, las instalaciones, el equipo, la operación y el mantenimiento de un PWS con el fin de evaluar la idoneidad de dicha fuente, instalaciones, equipo, operación y mantenimiento para producir y distribuir agua potable segura".[5] De conformidad con los requisitos reglamentarios pertinentes, los estados deben realizar inspecciones sanitarias periódicas de los PWS.[6] La EPA interpreta los requisitos reglamentarios relacionados con la realización de inspecciones sanitarias para exigir que cuando un PWS utilice tecnología operativa, como un sistema de control industrial (ICS), como parte del equipo o la operación de cualquier componente requerido[7] de una inspección sanitaria, la inspección sanitaria de ese PWS

[5] 40 CFR § 141.2
[6] 40 CFR §§ 141.2, 142.16(b)(3), 142.16(o)(2).
[7] 40 CFR § 142.16(b)(3) y (o)(2) [los componentes requeridos figuran en el anexo]

debe incluir una evaluación de la idoneidad de la seguridad cibernética de esa tecnología operativa para producir y distribuir agua potable segura.

Un sistema de control industrial es un sistema de información utilizado para controlar procesos industriales como la fabricación, la gestión de productos, la producción y la distribución. Los ICS incluyen sistemas de control de supervisión y adquisición de datos que se utilizan para controlar los activos dispersos geográficamente, así como los sistemas de control distribuido y los sistemas de control más pequeños que utilizan controladores lógicos programables para monitorear los procesos localizados.[8]

En consecuencia, durante una inspección sanitaria de un PWS, los estados deben hacer lo siguiente para cumplir con el requisito de realizar una inspección sanitaria:

(1) Si el PWS usa un ICS u otra tecnología operativa como parte del equipo o la operación de cualquier componente requerido de la inspección sanitaria, entonces el estado debe evaluar la idoneidad de la seguridad cibernética de esa tecnología operativa para producir y distribuir agua potable segura.

(2) Si el estado determina que una deficiencia en la seguridad cibernética identificada durante una inspección sanitaria es significativa, entonces el estado debe usar su autoridad para exigir que el PWS aborde la deficiencia significativa.[9]

La EPA ha determinado que las deficiencias significativas incluyen, entre otros, "defectos en el diseño, el funcionamiento o el mantenimiento, o una falla o funcionamiento defectuoso de las fuentes, el tratamiento, el almacenamiento o el sistema de distribución que el estado determina que están causando, o tienen potencial para causar, la introducción de contaminación en el agua suministrada a los consumidores".[10] En cuanto a la seguridad cibernética, las deficiencias significativas deben incluir la ausencia de una práctica o un control, o la presencia de una vulnerabilidad, que tenga un alto riesgo de ser explotada, ya sea directa o indirectamente, para comprometer una tecnología operativa usada en el tratamiento o la distribución de agua potable.

Como se describe en la sección 3, los estados pueden cumplir con la obligación de evaluar la seguridad cibernética a través de diferentes enfoques realizados en el marco de sus programas de inspecciones sanitarias. Alternativamente, pueden cumplir con este requisito utilizando un programa existente o estableciendo uno nuevo fuera de las inspecciones sanitarias que no sea menos estricto que las regulaciones federales e implique identificar y abordar las deficiencias significativas en las prácticas de seguridad cibernética en el PWS.[11]

---

[8] Centro de Recursos de Seguridad Informática del NIST, https://csrc.nist.gov/glossary/term/ics

[9] 40 CFR § 142.16(b)(1)-(3) y (o)(1)-(2)

[10] 40 CFR § 142.16(o)(2)(iv)

[11] De conformidad con la sección 1413 de la SDWA (42 U.S.C. § 300g-2) no es necesario que los estados con responsabilidad principal de hacer cumplir las normas (primacía) adopten regulaciones de agua potable idénticas a las regulaciones nacionales primarias de agua potable de la EPA. Más bien, los estados con primacía deben adoptar regulaciones de agua potable que no sean menos estrictas que las regulaciones nacionales primarias de agua potable de la EPA, lo que significa que estos estados tienen cierto grado de flexibilidad para lograr y mantener la primacía.

Los estados conservan la flexibilidad en las inspecciones sanitarias en cuanto a la forma en que evalúan los PWS, identifican las deficiencias significativas y exigen que los PWS las aborden. Esta interpretación se aplica a todos los estados, territorios y tribus que tienen jurisdicción sobre los PWS. Durante cualquier período en el que un gobierno estatal, territorial o tribal no tenga la responsabilidad principal de hacer cumplir las normas de conformidad con la sección 1413 de la Ley de Agua Potable Segura (SDWA), el término "estado" significa el administrador regional de la EPA de EE. UU. Como se indicó anteriormente, el uso de "estado" en esta guía abarca esta definición.

3.0 ¿Qué enfoques pueden usar los estados para incluir la seguridad cibernética en las inspecciones sanitarias de los PWS?

La EPA reconoce que varios estados ya han establecido programas para evaluar las prácticas de seguridad cibernética de los PWS y ayudar a los PWS a protegerse contra las amenazas cibernéticas. Otros estados pueden tener menos capacidad para ayudar a las comunidades lo suficiente en la creación de protecciones contra las amenazas cibernéticas. Para dar cuenta de las diferencias entre los estados en cuanto a su capacidad y competencia, la EPA brinda información sobre diferentes enfoques que los estados podrían emplear para evaluar la seguridad cibernética en los PWS. Además, los estados pueden querer disponer de flexibilidad para usar diferentes enfoques según las circunstancias de los PWS individuales, así como para pasar de un enfoque a otro a medida que la capacidad y la competencia cambian con el tiempo.

3.1. Opción 1: autoevaluación del PWS o evaluación de terceros de las prácticas de seguridad cibernética

Los estados que tengan o establezcan la autoridad requerida pueden exigir a los PWS que realicen una autoevaluación de las prácticas de seguridad cibernética con el fin de identificar las brechas de seguridad cibernética (es decir, la ausencia de prácticas o controles de seguridad cibernética recomendados o la presencia de vulnerabilidades).

Opción 1.a. Autoevaluación. Los PWS podrían realizar la evaluación utilizando un método del Gobierno o del sector privado aprobado por el estado, como los del Departamento de Seguridad Nacional (DHS), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA),12 el Instituto Nacional de Estándares y Tecnología (NIST),13 la American Water Works Association

[12] CISA *Cyber Resilience Review (Revisión de resiliencia cibernética de la CISA),* https://www.cisa.gov/uscert/resources/assessments

[13] NIST *Cybersecurity Framework (Marco de seguridad cibernética),* https://www.nist.gov/cyberframework

(AWWA),[14] la Organización Internacional de Normalización (ISO)[15] y la Sociedad Internacional de Automatización/Comisión Electrotécnica Internacional (ISA/IEC).[16] En la sección 5 y el apéndice A de esta guía, la EPA ha proporcionado una lista de verificación opcional que los PWS (o los estados) pueden usar para realizar una evaluación de las prácticas y los controles de seguridad cibernética recomendados.

Opción 1.b. Evaluación de terceros. De forma alternativa, un PWS podría someterse a una evaluación de las prácticas de seguridad cibernética por parte de un tercero, como el Programa de Evaluación de la Seguridad Cibernética del Sector del Agua de la EPA[17] u otro proveedor de asistencia técnica del Gobierno o del sector privado aprobado por el estado. La EPA está ampliando su capacidad para ayudar a los estados y los PWS a realizar evaluaciones.

En virtud de las opciones 1.a y 1.b, la evaluación de seguridad cibernética para el PWS —ya sea una autoevaluación o una realizada por un tercero— debe completarse antes de la inspección sanitaria, ponerse a disposición de los inspectores sanitarios del estado y, luego, actualizarse para reflejar los cambios en las prácticas de seguridad cibernética o la tecnología operativa antes de las inspecciones sanitarias posteriores. Durante la inspección sanitaria, el inspector del estado debe confirmar la finalización de la evaluación y determinar si las brechas de seguridad cibernética identificadas son deficiencias significativas. Como se describe en la sección 7, esta guía proporciona ejemplos y recomendaciones para que los estados consideren cuando identifiquen una deficiencia significativa de seguridad cibernética. Además, los estados y los PWS pueden solicitarle asistencia técnica a la EPA una vez que se identifiquen las brechas de seguridad cibernética.

Los estados también pueden exigir a los PWS que desarrollen planes de mitigación de riesgos de seguimiento para abordar las brechas de seguridad cibernética identificadas durante la evaluación, incluidas específicamente las deficiencias significativas que indique el estado. En el plan de mitigación de riesgos, se indicarán las acciones y los cronogramas de mitigación planificados. El estado revisará el plan de mitigación de riesgos durante la inspección sanitaria, se asegurará de que el PWS esté tomando las medidas necesarias para abordar las deficiencias significativas designadas por el estado, y se ofrecerá a identificar recursos adicionales que los PWS podrían usar para abordar esas brechas.

Los PWS deben completar el plan de mitigación de riesgos antes de su inspección sanitaria y actualizarlo, según sea necesario, antes de las inspecciones sanitarias posteriores. En esta guía, se incluyen las acciones recomendadas para abordar las brechas de seguridad cibernética, y la EPA ofrece una plantilla para un plan de mitigación

[14] AWWA, *Cybersecurity Assessment Tool and Guidance (Herramienta y guía de evaluación de la seguridad cibernética)*, https://www.awwa.org/Resources-Tools/Resource- Topics/Risk-Resilience/Cybersecurity-Guidance

[15] ISO, *27001 Information Security Management (Gestión de la seguridad de la información de la ISO)*, https://www.iso.org/isoiec-27001-information-security.html

[16] ISA/IEC, *62443 series of standards (Serie de normas 62443 de la ISA/IEC)*, https://www.isa.org/standards-and-publications/isa-standards/isa-iec- 62443-series-of-standards

[17] EPA *Water Sector Cybersecurity Evaluation Program (Programa de Evaluación de la Seguridad Cibernética del Sector del Agua de la EPA)*, https://www.epa.gov/waterriskassessment/forms/epas- water-sector-cybersecurity-evaluation-program

de riesgos en https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water- sector. La plantilla incluye campos para que un PWS describa la acción de mitigación planificada, la fecha de finalización prevista, la parte responsable, el estado actual y las notas explicativas. También está disponible la asistencia técnica de la EPA para ayudar a los estados y PWS con respecto a las acciones y los planes de mitigación de los riesgos de seguridad cibernética.

3.2 Opción 2: evaluación del estado de las prácticas de seguridad cibernética durante la inspección sanitaria

Los estados pueden optar por que los inspectores evalúen las prácticas de seguridad cibernética directamente durante una inspección sanitaria de un PWS para identificar las brechas en la seguridad cibernética y determinar si alguna de esas debería designarse como una deficiencia significativa. Este enfoque es consistente con la forma en que los estados realizan inspecciones sanitarias de otros componentes de las operaciones de los PWS. En función de esta opción, el estado, en lugar del PWS o de un tercero, realizaría la evaluación de seguridad cibernética y ordenaría al PWS que aborde cualquier deficiencia significativa que identifique el estado. La capacitación y la asistencia técnica de la EPA para evaluar la seguridad cibernética en las inspecciones sanitarias de los PWS también están disponibles para ayudar a los estados que adoptan este enfoque.

3.3 Opción 3: programa alternativo del estado para la seguridad cibernética del sistema de agua

Varios estados tienen programas en función de los cuales los PWS evalúan las brechas de seguridad cibernética (que podrían llamarse brechas de seguridad, vulnerabilidades o su equivalente) en sus prácticas actuales que podrían afectar el agua potable segura y, posteriormente, implementan controles para abordar esas brechas. Por ejemplo, una agencia de seguridad nacional del estado puede tener un programa de seguridad cibernética que cubra toda la infraestructura crítica del estado. Otro ejemplo es una agencia de gestión de emergencias del estado que realiza la evaluación de seguridad cibernética de los PWS en lugar de, o en colaboración con, la agencia del estado responsable del programa de supervisión del PWS.

Los estados que actualmente tienen o desarrollan dichos programas pueden usarlos como alternativas a la incorporación de la seguridad cibernética en las inspecciones sanitarias de los PWS. Los PWS que prestan servicio a comunidades rurales con poblaciones de menos de 10 000 habitantes pueden recurrir a proveedores de asistencia técnica financiados por la división de Desarrollo Rural (RD) del Departamento de Agricultura de EE. UU. (USDA). Es posible que estas comunidades ya tengan que cumplir requisitos respecto del análisis de seguridad cibernética como parte de los términos de un préstamo y de una subvención del sector de RD del USDA.

Para ser al menos tan estrictos como una inspección sanitaria, los inspectores del estado deben asegurarse de que los programas alternativos del estado identifiquen efectivamente las brechas de seguridad cibernética (o equivalente) a través de una evaluación, y que los PWS aborden las deficiencias significativas designadas por el estado. Además, la evaluación de seguridad cibernética realizada conforme a un programa alternativo debe llevarse a cabo al menos con la misma frecuencia que la inspección sanitaria requerida para el PWS (por lo general, 3 o 5 años).

3.4. Cambios en el mantenimiento de registros e informes del estado

Debido a que el memorándum no cambia el *Código de Regulaciones Federales*, no requiere que los estados revisen sus programas de primacía del estado aprobados.[18] Si el estado aprueba a un agente que no sea el estado para realizar el componente de seguridad cibernética de una inspección sanitaria en un PWS, como se describe en la opción 1, debe tener una lista de los agentes aprobados.[19] Los estados deben incluir la seguridad cibernética en su evaluación anual del programa estatal para realizar inspecciones sanitarias que ellos mismos presentan a la EPA.[20] En cuanto a los sistemas de agua subterránea, los estados deben tener los registros de los avisos escritos de las deficiencias significativas y la confirmación de que se ha corregido una deficiencia significativa.[21] Los estados deben informar a la EPA la fecha en que finalizó una acción correctiva en un sistema de agua subterránea.[22] Los estados no están obligados a informar la deficiencia significativa en sí a la EPA.

4.0 Soporte técnico para la seguridad cibernética en inspecciones sanitarias del PWS

Además de esta guía, la EPA brinda capacitación y asistencia técnica, como se describe a continuación, para ayudar a los estados y los PWS a abordar la seguridad cibernética en las inspecciones sanitarias. Aquí encontrará más información sobre estos recursos, así como material adicional, como preguntas frecuentes, hojas informativas y listas de posibles programas de financiación: https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector. En la sección 4.3 a continuación, figuran los recursos adicionales que pueden ayudar a los estados y PWS a evaluar la seguridad cibernética y abordar las deficiencias.

4.1. Capacitación

En 2023, la EPA tiene pensado ofrecer capacitación para los estados y los PWS sobre la evaluación de la seguridad cibernética en las inspecciones sanitarias. Al igual que en esta guía, la capacitación abordará los enfoques para evaluar las prácticas de seguridad cibernética en los PWS, lo que incluye la identificación de las brechas y las posibles deficiencias significativas, las acciones que los PWS podrían seguir para cerrar las brechas de seguridad cibernética, la protección de la información, la asistencia técnica disponible de la EPA y otras organizaciones del sector público y privado, y la potencial financiación.

La capacitación se impartirá virtualmente y se dejarán a disposición las grabaciones de estas. La capacitación específica para los estados también se ofrecerá en persona. Esta formación específica se llevará a cabo por separado

[18] 40 CFR § 142.12
[19] 40 CFR § 142.14(a)(5)(ii)(F)
[20] 40 CFR § 142.15(c)(5)
[21] 40 CFR § 142.17(d)(i) y (iii)
[22] 40 CFR § 142.15(c)(7)(ii)

para los estados en cada región de la EPA. En cuanto a los PWS, la capacitación se llevará a cabo a nivel nacional. En todas las capacitaciones, la EPA hará todo lo que esté a su alcance para garantizar la aprobación del estado de las unidades/los créditos de educación continua (CEC/CEU).

4.1 Asistencia técnica

La EPA ha establecido el *Programa de Asistencia Técnica en Seguridad Cibernética para el Sector del Agua.* De conformidad con este programa, los estados y los PWS pueden enviar preguntas o solicitar una consulta con un experto en la materia (SME) con respecto a la seguridad cibernética en las inspecciones sanitarias de los PWS, como identificar si una brecha de seguridad cibernética es una deficiencia significativa o seleccionar las acciones de mitigación de riesgos apropiadas. La EPA sugiere que el SME responda dentro de los dos días hábiles. Toda la asistencia será a distancia (por teléfono o por correo electrónico según corresponda). El servicio de asistencia técnica no será una línea de emergencia para denunciar incidentes cibernéticos y no será un recurso para la respuesta a incidentes cibernéticos ni medidas de recuperación (para estos asuntos, se dirigirá a los usuarios al contacto federal correspondiente). Acceda a este servicio de asistencia técnica aquí: https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity- evaluation-program.

El *Programa de Evaluación de la Seguridad Cibernética del Sector del Agua* de la EPA está disponible para evaluar las prácticas de seguridad cibernética en los PWS. La evaluación se regirá por la lista de verificación en el documento de orientación *Evaluating Cybersecurity in PWS Sanitary Surveys (Evaluación de la seguridad cibernética en las inspecciones sanitarias de los PWS)* (apéndice A). Luego de la evaluación, el PWS recibirá un informe con respuestas a las preguntas de la lista de verificación en el que se mostrarán las brechas en la seguridad cibernética, incluidas las posibles deficiencias significativas. El PWS debe proporcionar este informe al estado para que lo revise durante la inspección sanitaria, como se explica en la opción 1 de la sección 3 anterior. Para participar en este programa, el PWS debe registrarse en https://www.epa.gov/waterriskassessment/forms/epas-water-sector-cybersecurity- evaluation-program.

4.2 Recursos adicionales

A continuación, se encuentran los recursos técnicos y financieros adicionales que pueden ayudar a los estados y a los PWS a evaluar la seguridad cibernética durante las inspecciones sanitarias.

Recursos técnicos

- En la sección 6 de esta guía, figuran los ejemplos de los métodos del sector privado y gubernamental, además de los de la EPA, que pueden usarse para evaluar las prácticas de seguridad cibernética en los PWS e identificar las acciones para abordar las brechas de seguridad cibernética.
- El *Marco de seguridad cibernética*[23] del NIST es un marco voluntario integral basado en estándares, pautas y prácticas existentes para reducir los riesgos cibernéticos

[23] https://www.nist.gov/cyberframework

en la infraestructura fundamental. El NIST ofrece orientación y recursos para ayudar a los propietarios y operadores de infraestructura crítica a usar el *Marco de seguridad cibernética* para administrar sus riesgos cibernéticos.

- La CISA del DHS es una fuente principal de recursos para la seguridad cibernética de la infraestructura crítica. La CISA ofrece una amplia gama de herramientas, orientación y servicios para fortalecer la seguridad y la resiliencia de las instalaciones de infraestructura crítica contra los ataques cibernéticos.[24] Por ejemplo, los productos de la CISA pueden ayudar a los PWS a identificar vulnerabilidades de seguridad cibernética, desarrollar estrategias proactivas de mitigación que reduzcan el riesgo de la seguridad cibernética de la tecnología operativa y tomar medidas para contrarrestar las amenazas generalizadas como el ransomware.
- Los asesores de seguridad cibernética (CSA) de la CISA, que se encuentran en las diez oficinas regionales de la CISA,[25] ofrecen asistencia de seguridad cibernética a los propietarios y los operadores de la infraestructura crítica y a los gobiernos estatales, locales, tribales y territoriales. Los CSA se desempeñan como enlaces con los programas cibernéticos de la CISA, junto con otros recursos públicos y privados. Los CSA pueden ayudar con la preparación cibernética, las evaluaciones y los recursos de protección, la asociación en el desarrollo público-privado, y la coordinación y el apoyo de incidentes cibernéticos.
- El programa de RD del USDA, Circuit Rider, brinda asistencia técnica, incluido el análisis de seguridad cibernética, a los sistemas de agua rurales que prestan servicio a 10 000 personas o menos. [26] Los responsables de los sistemas rurales de abastecimiento de agua también pueden solicitar asistencia de la oficina local de Servicios Públicos Rurales del USDA o de la asociación estatal de la National Rural Water Association (NRWA). Circuit Rider brinda servicio en todos los estados y territorios.
- El Centro de análisis e intercambio de información (ISAC)[27] sobre el Agua es una fuente de datos, estudios de casos y análisis relacionados con las amenazas a la seguridad del agua, incluido el delito cibernético, y proporciona recursos para respaldar las iniciativas de respuesta, mitigación y resiliencia.
- El ISAC multiestatal respalda el intercambio de información para mejorar la seguridad cibernética general de los gobiernos estatales, locales, tribales y territoriales, ayuda con la respuesta y la resolución de los incidentes cibernéticos y emite avisos con información procesable para mejorar la seguridad cibernética.[28]

[24] https://www.cisa.gov/cybersecurity
[25] https://www.cisa.gov/cisa-regions
[26] hhttps://www.rd.usda.gov/programs-services/water-environmental-programs/circuit-rider-program- technical-assistance-rural-water-systems
[27] https://www.waterisac.org/
[28] https://www.cisecurity.org/ms-isac

- Las asociaciones privadas del sector del agua, incluidas la AWWA[29] y la NRWA[30,] ofrecen educación, orientación y métodos sobre seguridad cibernética para evaluar los riesgos de seguridad cibernética y priorizar las mejoras en seguridad cibernética dirigidas específicamente a los PWS.

Recursos financieros

- La EPA administra el fondo de préstamos y las reservas del Fondo Rotatorio Estatal de Agua Potable (DWSRF), que pueden usarse para apoyar programas del estado y comunidades con controles de seguridad cibernética.[31]
- El Programa de Resiliencia y Sostenibilidad de la Infraestructura de Sistemas de Agua Potable Medianos y Grandes de la EPA es un nuevo programa de subvenciones para sistemas públicos de agua que prestan servicio a más de 10 000 personas para apoyar proyectos que aumentan la resiliencia a los peligros naturales, las vulnerabilidades de seguridad cibernética o los eventos climáticos extremos.
- Los Programas Medioambientales y de Agua del Servicio de Servicios Públicos Rurales del USDA brindan préstamos, subvenciones y garantías de préstamos, así como asistencia técnica, a los PWS en comunidades rurales de 10 000 personas o menos para infraestructura y mejoras de infraestructura, lo cual incluye actualizaciones relacionadas con la seguridad cibernética.[32]
- El Programa de Subsidios para Seguridad Cibernética Estatal y Local del DHS, administrado conjuntamente por la CISA y la Agencia Federal para el Manejo de Emergencias (FEMA), ayuda a los gobiernos estatales, locales y territoriales de todo el país a abordar los riesgos y las amenazas de seguridad cibernética que enfrentan los sistemas de información que poseen o los que son operados en su beneficio.[33,34]

5.0 Lista de verificación de seguridad cibernética de la EPA para las inspecciones sanitarias del sistema público de agua

5.1. ¿Cuál es el propósito de esta lista de verificación?

La lista de verificación de la EPA (apéndice A) proporciona un método para evaluar la seguridad cibernética de la tecnología operativa, incluidas las redes de tecnología de la información que están conectadas a la tecnología operativa, en un PWS durante una inspección sanitaria. Las preguntas y las acciones recomendadas para abordar las deficiencias que figuran en la lista de verificación de la EPA se extrajeron directamente de los *Objetivos de rendimiento de la seguridad cibernética intersectorial de 2022 de la CISA*.[35]

[29] https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance
[30] https://nrwa.org/issues/cybersecurity/
[31] https://www.epa.gov/sites/default/files/2019-10/documents/cybersecurity_fact_sheet_final.pdf
[32] https://www.rd.usda.gov/programs-services/water-environmental-programs
[33] https://www.cisa.gov/cybergrants
[34] https://www.epa.gov/system/files/documents/2022-12/221121-SLCGP_508c.pdf
[35] https://www.cisa.gov/cpg

En esta lista de verificación de la EPA, se redactaron los objetivos de rendimiento de la seguridad cibernética (CPG) en un formato de preguntas simplificado para facilitar su uso en la evaluación de un PWS.

Las preguntas de la lista de verificación de la EPA están pensadas para identificar brechas de seguridad cibernética o vulnerabilidades potenciales en los controles y las prácticas de seguridad cibernética actuales. Se alienta a los PWS a utilizar los recursos y la asistencia técnica en las hojas informativas del apéndice B de esta guía para abordar las brechas y reducir el riesgo de que un ataque cibernético pueda comprometer sus operaciones.

Una respuesta negativa a una pregunta de la lista de verificación no pretende, por sí misma, indicar una deficiencia significativa en un PWS. Las posibles deficiencias significativas se mencionan en la sección 7 de esta guía. El estado es responsable de determinar si designa una brecha de seguridad cibernética como una deficiencia significativa. En general, los estados deben permitir que los PWS tengan tiempo suficiente para corregir las brechas de seguridad cibernética identificadas en las evaluaciones y solo considerar emitir una deficiencia significativa cuando un PWS no logra corregir una vulnerabilidad crítica.

5.2. Lista de verificación

La lista de verificación se encuentra en el apéndice A.

6.0 Alternativas recomendadas a la lista de verificación de la EPA

El uso de la Lista de verificación de la EPA descrita en la sección 5 y provista en el apéndice A de esta guía durante una inspección sanitaria es opcional. Alternativamente, la evaluación de seguridad cibernética durante una inspección sanitaria de PWS se puede realizar con otros métodos de evaluación gubernamentales o del sector privado aprobados por el estado, como los de la CISA,[36] el NIST,[37] la AWWA,[38] la ISO,[39] y la ISA/IEC.[40]

7.0 Posibles deficiencias significativas

Según lo determinado por el estado,[41] una deficiencia significativa durante una inspección sanitaria de PWS es una deficiencia que hará que este implemente acciones de cumplimiento si no se corrige dentro del plazo indicado.

---

[36] CISA *Cyber Resilience Review (Revisión de resiliencia cibernética de la CISA),* https://www.cisa.gov/uscert/resources/assessments

[37] NIST *Cybersecurity Framework (Marco de seguridad cibernética),* https://www.nist.gov/cyberframework

[38] AWWA, *Cybersecurity Assessment Tool and Guidance (Herramienta y guía de evaluación de la seguridad cibernética),* https://www.awwa.org/Resources-Tools/Resource- Topics/Risk-Resilience/Cybersecurity-Guidance

[39] ISO, *27001 Information Security Management (Gestión de la seguridad de la información 27001 de la ISO)*, https://www.iso.org/isoiec-27001-information-security.html

[40] ISA/IEC *62443 series of standards (Serie de normas 62443 de la ISA/IEC),* https://www.isa.org/standards-and-publications/isa-standards/isa-iec- 62443-series-of-standards

[41] Incluye tribus, territorios y regiones de la EPA cuando se ejerce la autoridad principal de aplicación de un sistema público de agua.

En la sección 2, se presenta la definición reglamentaria de la EPA de deficiencia significativa y se aplica a la seguridad cibernética en el contexto de una inspección sanitaria de PWS (la ausencia de un control o práctica que tiene un alto riesgo de ser usada para comprometer un activo tecnológico operativo utilizado en el tratamiento o la distribución de agua potable). A continuación, la EPA sugiere brechas específicas de seguridad cibernética de la Lista de verificación que se encuentra en el apéndice A para que los estados las consideren como posibles deficiencias significativas. Para determinar estas brechas, la EPA consideró los siguientes factores:

- alto riesgo y antecedentes de explotación en el sector del agua u otros sectores de infraestructura fundamental a través de tácticas, técnicas y procedimientos ampliamente utilizados para ataques cibernéticos;
- viabilidad técnica para que la mayoría de los PWS las aborden sin gastos de capital significativos; y
- plazo de implementación a corto plazo para corregirlas.

Los estados conservan su autoridad y criterio actuales para determinar cuándo una brecha de seguridad cibernética identificada durante una inspección sanitaria o un proceso alternativo equivalente debe designarse como una deficiencia significativa. Los estados también aprueban las acciones y los plazos para que los PWS aborden las deficiencias significativas. Como se indicó anteriormente, los estados pueden otorgar a los PWS el tiempo suficiente para abordar las brechas de seguridad cibernética identificadas en las evaluaciones y solo emitir una deficiencia significativa cuando un PWS no corrige una vulnerabilidad crítica.

Las posibles deficiencias significativas sugeridas a continuación figuran con su número correspondiente de la Lista de verificación de la EPA proporcionada en el apéndice A, lo cual corresponde con los *CPG intersectoriales de 2022 de la CISA*.[42]

Seguridad de cuentas

- El PWS no cambia las contraseñas predeterminadas en los activos de tecnología operativa (OT) cuando es factible NI implementa controles de compensación (p. ej., segmentación o aislamiento del activo, mayor monitoreo de eventos de seguridad) cuando no es factible cambiar la contraseña predeterminada de los activos de OT. (Lista de verificación/CPG 1.2)
- El PWS no utiliza la autenticación de múltiples factores para el acceso remoto a las redes de OT. (Lista de verificación/CPG 1.3)
- El PWS no exige una longitud mínima para las contraseñas. (Lista de verificación/CPG 1.4)
- El PWS no revoca las credenciales de acceso a sus redes cuando un empleado se va o cuando un usuario previamente autorizado ya no requiere acceso. (Lista de verificación/CPG 1.7)

[42] https://www.cisa.gov/cpg

Seguridad de dispositivos

- El PWS no mantiene un inventario actualizado de todos sus activos de OT (incluidos todos los activos de tecnología de la información [IT] conectados). (Lista de verificación/CPG 2.3)
- El PWS no conserva la documentación de configuración de sus activos de OT y IT. (Lista de verificación/CPG 2.5)

Gobernanza y formación

- El PWS no tiene una función, un puesto o un cargo designados que se encarguen de todas las actividades de seguridad cibernética de PWS. (Lista de verificación/CPG 4.1)
- El PWS no brinda capacitación anual en seguridad cibernética para todo el personal. (Lista de verificación/CPG 4.3)

Gestión de vulnerabilidades

- El PWS no mitiga las vulnerabilidades conocidas mediante la instalación de firmware y parches de software en un plazo dependiente de los riesgos (primero los activos críticos o más expuestos) NI implementa controles de compensación (p. ej., segmentación o aislamiento del activo, mayor monitoreo de eventos de seguridad) donde la aplicación de parches no es factible. (Lista de verificación/CPG 5.1)
- El PWS no ha eliminado todas las conexiones de activos de OT a la Internet pública, a menos que se requiera explícitamente para las operaciones. (Lista de verificación/CPG 5.5)

Cadena de suministro/terceros

- El PWS no incluye requisitos ni preguntas de seguridad cibernética en sus documentos de adquisición de activos y servicios de OT, que luego se consultan para la selección de proveedores (Lista de verificación/CPG 6.1).
- El PWS no estipula en sus documentos de adquisición que los vendedores o proveedores de servicios deban notificar a PWS sobre incidentes de seguridad y vulnerabilidades confirmadas de manera oportuna. (Lista de verificación/CPG 6.2/6.3).

Respuesta y recuperación

- El PWS no tiene establecido un plan de respuesta a incidentes de seguridad cibernética de OT. (Lista de verificación/CPG 7.2)
- El PWS no realiza una copia de seguridad de todos los sistemas necesarios para las operaciones (p. ej., configuraciones de red, lógica del controlador lógico programable [PLC], diagramas de ingeniería) con regularidad. (Lista de verificación/CPG 7.3)
- El PWS no almacena las copias de seguridad por separado de los sistemas de origen. (Lista de verificación/CPG 7.3)

- El PWS no conserva la documentación actualizada (p. ej., diagramas) de las conexiones entre todos los componentes de red de las redes de OT (es decir, arquitectura o topología de la red). (Lista de verificación/CPG 7.4)

Las hojas informativas numeradas en esta guía (apéndice B) tienen información que puede ayudar a los PWS a resolver deficiencias significativas mediante la implementación de los controles de seguridad cibernética descritos.

8.0 ¿Cómo deben los estados proteger la información confidencial sobre la seguridad cibernética de los PWS?

Es posible que sea necesario ocultar del público la información sobre prácticas y vulnerabilidades de seguridad cibernética específicas en los PWS debido a la posibilidad de que se use para facilitar una intrusión cibernética o un ataque en el PWS.

En algunos casos, las oficinas regionales de la EPA realizan inspecciones sanitarias como agencia de primacía para un estado o área en particular (p. ej., Wyoming, el Distrito de Columbia, la mayoría de las tribus indígenas). La EPA también puede realizar evaluaciones de seguridad cibernética a través del Programa de Evaluación de la Seguridad Cibernética del Sector del Agua (consulte la sección 3.1). La Agencia planea hacer valer las exenciones aplicables de la Ley de Libertad de Información (FOIA) para proteger las partes confidenciales de cualquier informe de inspección sanitaria o evaluación de seguridad cibernética de PWS en poder de la EPA, incluidas las partes que se ocupan de las prácticas de seguridad cibernética de un PWS si dicho informe se solicita de conformidad con la FOIA. Las exenciones aplicables conforme a la FOIA para proteger dicha información pueden incluir la exención 4 (información comercial confidencial o CBI) y la exención 7(f) (registros policiales cuya divulgación podría razonablemente esperarse que pusiera en peligro la vida o la seguridad física de cualquier individuo).

En cuanto a las inspecciones sanitarias realizadas por un gobierno estatal, tribal o territorial, las leyes aplicables de la entidad gubernamental que posee el informe regirán la protección de la información confidencial de seguridad cibernética de la divulgación pública. La mayoría de los estados han adoptado leyes de protección de la información como la FOIA de conformidad con la ley estatal,[43] y la EPA recomienda que los estados protejan dicha información confidencial si se solicita en la medida permitida por la ley estatal. Los requisitos del estado para notificar a la EPA información relacionada con la evaluación de la seguridad cibernética en las inspecciones sanitarias se analizan en la sección 3.4 anterior.

En el apéndice del memorándum, se incluyen recomendaciones para los estados sobre potenciales enfoques para identificar y segregar la información de seguridad cibernética en los informes de inspecciones sanitarias que no debe divulgarse públicamente.

---

[43] AWWA, *Protecting the Water Sector's Critical Infrastructure Information, Analysis of State Laws (Protección de la información de la infraestructura crítica del sector del agua; análisis de leyes estatales)*, https://www.awwa.org/Portals/0/AWWA/Government/ProtectingtheWaterSectorsCriticalInfrastructureInformation.pdf

Por ejemplo, los estados a los que les preocupa su autoridad para proteger la información confidencial sobre seguridad cibernética de la divulgación pública pueden tomar las siguientes medidas mientras se respeta la ley estatal vigente:

- Los inspectores sanitarios pueden dejar a los PWS las evaluaciones de las prácticas de seguridad cibernética, la identificación de brechas de seguridad cibernética, los planes de mitigación y otra información confidencial. El estado no retendría esta información.
- Los informes oficiales de los inspectores podrían limitarse a confirmar que se realizó la evaluación de seguridad cibernética, indicar si se identificaron brechas (incluidas las deficiencias significativas), y plantear el cronograma de acciones correctivas si fuera necesario. La información sobre brechas específicas y deficiencias significativas se dejaría a los PWS (no se incluiría en el informe del estado ni quedaría en poder de este). El inspector del estado revisaría el progreso en la corrección de las deficiencias significativas durante los seguimientos virtuales o en el sitio.
- Cuando esté permitido, los inspectores podrían tomar notas detalladas sobre las vulnerabilidades de seguridad cibernética del PWS y la información relacionada en documentos internos no públicos que no estén sujetos a los requisitos de divulgación pública.

APÉNDICE A: Lista de verificación de seguridad cibernética de la EPA para las inspecciones sanitarias del sistema público de agua

1. **Seguridad de cuentas.** *¿Acaso el PWS hace lo siguiente?*

   1.1. ¿Detecta y bloquea reiterados intentos fallidos de inicio de sesión?

   Recomendación: cuando sea técnicamente factible, se debe notificar a los administradores del sistema después de una determinada cantidad de intentos de inicio de sesión fallidos consecutivos en un corto tiempo. En ese momento, los futuros intentos de inicio de sesión de la cuenta sospechosa deben bloquearse durante un tiempo determinado o hasta que un administrador los vuelva a habilitar.

   1.2. ¿Cambia las contraseñas predeterminadas?

   Recomendación: cuando sea factible, cambie todas las contraseñas predeterminadas del fabricante o proveedor antes de poner en servicio el equipo o el software.

   1.3. ¿Requiere la autenticación de múltiples factores (MFA) siempre que sea posible pero como mínimo para acceder de forma remota a las redes de tecnología operativa (OT) de PWS?

   Recomendación: implemente la MFA lo más que se pueda en las redes de IT y de OT. Como mínimo, se debe implementar la MFA para el acceso remoto a la red de OT.

   1.4. ¿Exige una longitud mínima para las contraseñas?

   Recomendación: cuando sea posible, implemente un requisito de longitud mínima para las contraseñas. La implementación puede ser a través de una política o controles administrativos configurados en el sistema.

   1.5. ¿Separa las cuentas del usuario y las que tienen privilegios (p. ej., administrador del sistema)?

   Recomendación: restrinja los privilegios del administrador del sistema para separar las cuentas de usuario solo para tareas administrativas y evalúe los privilegios administrativos periódicamente para asegurarse de que las personas que tienen estos privilegios aún los necesiten.

   1.6. ¿Solicita credenciales únicas y separadas para que los usuarios accedan a las redes de OT y de IT?

   Recomendación: requiera que un solo usuario tenga dos nombres de usuario y contraseñas diferentes; un conjunto se utilizará para acceder a la red de IT y el otro para acceder a la red de OT. Esto reduce el riesgo de que un atacante pueda moverse entre ambas redes utilizando un solo inicio de sesión.

1.7. ¿Deshabilita inmediatamente el acceso a una cuenta o red cuando ya no se requiere debido a que la persona se retiró, cambió de puesto, dejó de trabajar allí u otros factores?

Recomendación: tome todas las medidas necesarias para cancelar el acceso a cuentas o redes ante un cambio en el estado de una persona que hace que el acceso sea innecesario.

2. **Seguridad de dispositivos.** *¿Acaso el PWS hace lo siguiente?*

2.1. ¿Requiere aprobación antes de instalar o implementar un nuevo software?

Recomendación: solo permita a los administradores instalar software nuevo en un activo emitido por el PWS.

2.2. ¿Deshabilita las macros de Microsoft Office o un código incorporado similar de forma predeterminada en todos los activos?

Recomendación: deshabilite las macros incorporadas y el código ejecutable similar de forma predeterminada en todos los activos.

2.3. ¿Mantiene un inventario actualizado de todos los activos de red de OT y IT?

Recomendación: haga una revisión (no menos de una vez al mes) y un mantenimiento con regularidad de la lista de todos los activos de OT y IT con una dirección IP. Esto incluye equipos heredados (es decir, más antiguos) y de terceros.

2.4. ¿Prohíbe la conexión de hardware no autorizado (p. ej., dispositivos USB, unidades extraíbles, computadoras portátiles que llevan otras personas) a activos de OT y IT?

Recomendación: cuando sea factible, elimine, deshabilite o asegure los puertos físicos (p. ej., los puertos USB en una computadora portátil) para evitar que se conecten activos no autorizados.

2.5. ¿Mantiene la documentación actualizada que detalla la instalación y los ajustes (es decir, la configuración) de los activos críticos de OT y IT?

Recomendación: conserve la documentación precisa de la configuración original y actual de los activos de OT y IT, incluida la versión de software y de firmware.

3. **Seguridad de los datos.** *¿Acaso el PWS hace lo siguiente?*

3.1. ¿Recopila los registros de seguridad (p. ej., acceso al sistema y a la red, detección de malware) para usarlos tanto en la detección como en la investigación de incidentes?

Recomendación: recopile y almacene registros o datos de tráfico de red para poder detectar ataques cibernéticos e investigar actividades sospechosas.

3.2. ¿Protege los registros de seguridad contra el acceso no autorizado y la manipulación?

Recomendación: almacene los registros de seguridad en un sistema central o en una base de datos a la que solo puedan acceder los usuarios autorizados y autenticados.

3.3. ¿Utiliza un cifrado eficaz para mantener la confidencialidad de los datos en tránsito?

Recomendación: cuando envíe datos e información, utilice los estándares de cifrado de seguridad de la capa de transporte (TLS) o de la capa de sockets seguros (SSL).

3.4. ¿Utiliza el cifrado para mantener la confidencialidad de los datos confidenciales almacenados?

Recomendación: no almacene datos confidenciales, incluidas las credenciales (es decir, nombres de usuario y contraseñas) en texto sin formato.

4. **Gobernanza y formación.** *¿Acaso el PWS hace lo siguiente?*

4.1. ¿Tiene una función, un puesto o un cargo designados que se encarguen de la planificación, la obtención de recursos y la ejecución de las actividades de seguridad cibernética dentro del PWS?

Recomendación: identifique una función, un puesto o un cargo responsable de la seguridad cibernética dentro del PWS. Quien lo desempeñe estará a cargo de todas las actividades de seguridad cibernética de PWS.

4.2. ¿Tiene una función, un puesto o un cargo designados que se encarguen de la planificación, la obtención de recursos y la ejecución de las actividades de seguridad cibernética específicas de OT?

Recomendación: identifique una función, un puesto o un cargo del PWS responsable de garantizar la planificación, la obtención de recursos y la ejecución de actividades de seguridad cibernética específicas de OT.

4.3. ¿Proporciona al menos capacitación anual para todo el personal de PWS que aborde los conceptos básicos de seguridad cibernética?

Recomendación: lleve a cabo una capacitación básica anual en seguridad cibernética para todo el personal de PWS.

4.4. ¿Ofrece capacitación en seguridad cibernética específica de OT al menos una vez al año al personal que usa OT en sus funciones habituales?

Recomendación: brinde capacitación especializada en seguridad cibernética centrada en la OT a todo el personal que utiliza activos de OT.

4.5. ¿Ofrece oportunidades periódicas para fortalecer la comunicación y la coordinación entre el personal de OT y IT, incluidos los proveedores?

Recomendación: organice reuniones entre el personal de OT y IT para que todas las partes comprendan mejor las necesidades de seguridad de la organización y se fortalezcan las relaciones laborales.

5. **Gestión de vulnerabilidades.** *¿Acaso el PWS hace lo siguiente?*

5.1. ¿Coloca parches o mitiga de otro modo las vulnerabilidades conocidas dentro del plazo recomendado?

Recomendación: identifique y corrija las vulnerabilidades teniendo en cuenta los riesgos (p. ej., los activos fundamentales primero) lo más rápido posible.

5.2. Este número de control se incluye aquí para que corresponda con los CPG de la CISA, pero no se aplica a la mayoría de los PWS.

5.3. Este número de control se incluye aquí para que corresponda con los CPG de la CISA, pero no se aplica a la mayoría de los PWS.

5.4. ¿Se asegura de que los activos conectados a la Internet pública no expongan servicios explotables innecesarios (p. ej., protocolo de escritorio remoto)?

Recomendación: elimine los puertos y servicios expuestos innecesarios en los activos de cara al público y revíselos periódicamente.

5.5 ¿Elimina las conexiones entre sus activos de OT e Internet?

Recomendación: elimine las conexiones de activos de OT a la Internet pública, a menos que se requieran explícitamente para las operaciones.

5.6 Este número de control se incluye aquí para que corresponda con los CPG de CISA, pero no se aplica a la mayoría de los PWS.

6. **Cadena de suministro/terceros.** *¿Acaso el PWS hace lo siguiente?*

6.1. ¿Incluye la seguridad cibernética como criterio de evaluación para la adquisición de activos y servicios de OT?

Recomendación: incluya la seguridad cibernética como criterio de evaluación en la adquisición de bienes y servicios.

6.2/6.3 ¿Exige que todos los proveedores de OT y de servicios notifiquen al PWS sobre cualquier incidente de seguridad o vulnerabilidad en un determinado plazo dependiente de los riesgos?

Recomendación: exija a los vendedores y los proveedores de servicios que notifiquen al PWS sobre posibles incidentes de seguridad y vulnerabilidades dentro de un plazo estipulado indicado en los documentos y contratos de adquisición.

7. **Respuesta y recuperación.** *¿Acaso el PWS hace lo siguiente?*

7.1. ¿Tiene un procedimiento escrito para reportar incidentes de seguridad cibernética que indique el medio (p. ej., llamada telefónica, envío por Internet) y el destinatario (p. ej., Buró Federal de Investigaciones [FBI] u otras fuerzas del orden público, la CISA, reguladores estatales, WaterISAC, un proveedor de seguros cibernéticos)?[44]

Recomendación: documente el procedimiento a fin de informar incidentes de seguridad cibernética con prontitud para contribuir con la aplicación de la ley, recibir asistencia con la respuesta y la recuperación, y promover la conciencia del sector del agua sobre las amenazas de seguridad cibernética.

7.2. ¿Tiene un plan escrito de respuesta a incidentes de seguridad cibernética (IR) para escenarios de amenazas críticas (p. ej., desactivación o manipulación de sistemas de control de procesos, pérdida o robo de datos operativos o financieros, exposición de información confidencial), que se ponga en práctica y se actualice con regularidad?

Recomendación: desarrolle, ponga en práctica y actualice un plan de IR para los incidentes de seguridad cibernética que podrían afectar las operaciones de PWS. Realice simulacros para mejorar las respuestas a posibles incidentes cibernéticos.

7.3. ¿Hace una copia de seguridad de los sistemas necesarios para las operaciones (p. ej., configuraciones de red, lógica del PLC, diagramas de ingeniería, registros de personal) con regularidad, las almacena por separado de los sistemas de origen y las prueba periódicamente?

Recomendación: realice copias de seguridad de los sistemas de OT y IT fundamentales de PWS, guárdelas de manera segura y por separado, y pruébelas.

7.4. ¿Conserva la documentación actualizada que describe la topología de la red (es decir, las conexiones entre todos los componentes de la red) en las redes de OT y IT del PWS?

Recomendación: conserve una documentación completa y precisa de todas las topologías de redes de IT y OT del PWS para facilitar la respuesta y la recuperación ante incidentes.

[44] De conformidad con la Ley de Informes de Incidentes Cibernéticos de Infraestructura Fundamental de 2022, la CISA establecerá procedimientos que pueden aplicarse a los sistemas públicos de agua. Esta recomendación se revisará según sea necesario cuando se publiquen esos procedimientos.

8. **Otro.** *¿Acaso el PWS hace lo siguiente?*

8.1. ¿Segmentar las redes de OT y IT y denegar las conexiones a la red de OT de forma predeterminada, a menos que se permita explícitamente (p. ej., por dirección IP y puerto)?

Recomendación: requiera que las conexiones entre las redes de OT y IT pasen a través de un intermediario, como un cortafuegos, un servidor bastión, una caja de salto o una zona desmilitarizada, que se monitorea y registra.

8.2. ¿Tiene una lista de amenazas y tácticas, técnicas y procedimientos del adversario (TTP) de ataques cibernéticos relevantes para el PWS y tiene la capacidad de detectar instancias de amenazas clave?

Recomendación: reciba alertas de la CISA y mantenga la documentación de los TTP relevantes para el PWS.

8.3. ¿Usa controles de seguridad de correo electrónico para reducir las amenazas comunes basadas en correo electrónico, como la suplantación de identidad, el phishing y la intercepción?

Recomendación: asegúrese de que los controles de seguridad del correo electrónico estén habilitados en toda la infraestructura de correo electrónico corporativa.

APÉNDICE B: Hojas informativas de la lista de verificación

Seguridad de cuentas: detección de intentos de inicio de sesión fallidos (automatizados)

COSTO: **$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

1.1: ¿Acaso el PWS detecta y bloquea reiterados intentos fallidos de inicio de sesión? **Recomendación:** cuando sea técnicamente factible, se debe notificar a los administradores del sistema después de una determinada cantidad de intentos de inicio de sesión fallidos consecutivos en un corto tiempo. En ese momento, los futuros intentos de inicio de sesión de la cuenta sospechosa deben bloquearse durante un tiempo determinado o hasta que un administrador los vuelva a habilitar.

¿Por qué es importante este control?

Una técnica común que utilizan los atacantes para entrar a los sistemas de OT y IT es intentar "adivinar" el nombre de usuario y la contraseña de inicio de sesión. El ataque se puede lograr adivinando manualmente la contraseña de una cuenta, usando una lista de contraseñas comunes o a la fuerza. Con esta técnica, un atacante utiliza un enfoque de prueba y error para adivinar sistemáticamente las credenciales de inicio de sesión. El atacante envía combinaciones de nombres de usuario y contraseñas, generalmente utilizando una herramienta de descifrado de contraseñas automatizada y fácilmente disponible hasta que acierta. Bloquear a un atacante para que no siga tratando de adivinar las credenciales después de una determinada cantidad de intentos incorrectos puede detener este tipo de ataques. Sin bloquear los intentos de inicio de sesión, este ataque puede seguir en curso hasta que el atacante descifra la contraseña. Un descifrador de contraseñas puede ejecutarse durante horas, días y semanas y, finalmente, descifrar una contraseña a la fuerza, a menos que haya una política que impida que esto suceda.

Lineamientos adicionales

- Configure los sistemas para que notifiquen automáticamente (p. ej., mediante una alerta generada por computadora) a los equipos de seguridad o al administrador del sistema después de un número específico de intentos de inicio de sesión fallidos consecutivos en un breve período (p. ej., cinco intentos fallidos en menos de 2 minutos).
- Habilite los ajustes de bloqueo de cuenta en los sistemas correspondientes para evitar futuros intentos de inicio de sesión de la cuenta sospechosa durante un tiempo mínimo o hasta que el administrador del sistema vuelva a habilitarla.
- Registre y almacene la información de la alerta para su análisis. Use procedimientos de registro sólidos: en el registro, deben figurar el origen del suceso, la fecha, el nombre del usuario, la marca de tiempo, las direcciones de origen, las direcciones de destino y cualquier otra información útil que pudiera ayudar en una investigación forense.

Consejos de implementación

Según la versión de Windows que use un PWS, el administrador del sistema puede usar la política de seguridad local para restringir la cantidad de intentos de inicio de sesión. Para acceder a esta función, escriba "Local Security Policy" (Política de seguridad local) en el cuadro de búsqueda del menú de Inicio y haga clic en la aplicación Política de seguridad local. Una vez que se abra el panel del menú, haga clic en Account Policies (Políticas de la cuenta) para configurar los intentos de inicio de sesión y la duración del bloqueo.

Si un PWS utiliza un dominio de Microsoft con muchos sistemas y cuentas de usuario conectados a un solo dominio, puede administrar estos ajustes usando los objetos de directiva de grupo (GPO). El administrador del sistema puede habilitar los ajustes de la política de bloqueo de cuentas en la siguiente ubicación de la consola de administración de políticas de grupo: Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy (Configuración del equipo\Ajustes de Windows\Ajustes de seguridad\Políticas de cuenta\Directiva de bloqueo de cuentas). En el enlace de Referencia de los ajustes de la política de seguridad de Microsoft Windows a continuación, encontrará más detalles.

Cuando indique un umbral de bloqueo de inicio de sesión de la cuenta, asegúrese de que se haya configurado en un nivel adecuado en función de la importancia crítica del sistema (generalmente entre cinco y diez intentos). El nivel seleccionado debe proporcionar margen a los operadores hasta que ingresen las credenciales correctas, pero debe ser lo suficientemente sólido como para evitar la mayoría de los ataques a la fuerza.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte la página 39, Intentos fallidos de inicio de sesión (control AC-7), para obtener más información. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Punto de referencia de Microsoft Windows del Centro para la Seguridad en Internet (CIS): en este documento, se describe cómo implementar las acciones preventivas en sistemas basados en Microsoft Windows. La sección donde se aborda la política de bloqueo de cuentas comienza en la página 50. La implementación del seguimiento detallado se describe en la página 382.
https://www.cisecurity.org/benchmark/microsoft_windows_desktop

Referencia de los ajustes de la política de seguridad de Microsoft Windows: en esta página, se describe cómo configurar los ajustes de bloqueo de cuenta en los sistemas de Windows.
https://learn.microsoft.com/en- us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold

COSTO: **$**$$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

1.2: ¿Acaso el PWS cambia las contraseñas predeterminadas?

Recomendación: cuando sea factible, cambie todas las contraseñas predeterminadas del fabricante o proveedor antes de poner en servicio el equipo o el software.

¿Por qué es importante este control?

El hardware y el software listos para usar están diseñados para una fácil instalación y uso. Los ajustes predeterminados de fábrica a menudo incluyen contraseñas simples documentadas públicamente. Muchas veces, estas contraseñas predeterminadas son idénticas (compartidas) en todos los sistemas de un proveedor o en las líneas de productos. Por estos motivos, los PWS deben cambiar las contraseñas predeterminadas después de finalizadas la prueba, la instalación y la configuración iniciales. De lo contrario, los atacantes pueden obtener fácilmente contraseñas predeterminadas del manual del usuario de un producto y usar estas credenciales para acceder a los sistemas, ya sea localmente o por Internet, si el sistema de destino está conectado.

Lineamientos adicionales

- Desarrolle una política o un proceso aplicado en toda la organización que exija cambiar las contraseñas predeterminadas del proveedor o del fabricante en el hardware o software utilizado en el PWS.
- Si bien cambiar las contraseñas predeterminadas en el OT existente de un PWS puede requerir la ayuda de un proveedor o integrador calificado y puede no ser factible siempre, el PWS debe cambiar las credenciales predeterminadas de todo el hardware o software recientemente implementados.

Consejos de implementación

Muchos activos vienen con un nombre de usuario y una contraseña predeterminados que se pueden encontrar en la documentación del producto y en las listas compiladas disponibles en Internet. Los PWS deben revisar su inventario de activos existente e identificar cualquier activo que potencialmente podría haber venido con contraseñas predeterminadas. Estos activos pueden incluir hardware de red (p. ej., conmutadores de red, puntos de acceso inalámbrico, enrutadores de red); activos de comunicaciones (p. ej., radios); activos de OT (p. ej., PLC e interfaz hombre-máquina [HMI]); y aplicaciones de software en las que el fabricante o proveedor que instala la aplicación en el PWS establece contraseñas predeterminadas. El PWS debe revisar la documentación de estos activos, incluidos los manuales de instrucciones y las guías de configuración (comúnmente disponibles en el sitio web del proveedor), para identificar cualquier nombre de usuario o contraseña predeterminados. Una vez que el PWS identifica estas combinaciones de nombre de usuario y contraseña, el administrador del sistema debe intentar iniciar sesión con estas credenciales y, si lo logra, averiguar si puede cambiarlas sin afectar las operaciones del sistema. En los casos en que no sea factible cambiar las contraseñas predeterminadas, implemente y documente los controles de seguridad de compensación apropiados y supervise los registros del tráfico de red e intentos de inicio de sesión en esos activos.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: proporciona un enfoque proactivo y sistémico a fin de desarrollar y poner a disposición un conjunto integral de medidas de protección para todo tipo de plataformas informáticas. Consulte el control IA-5 (página 138) para obtener más información sobre la Gestión del autenticador. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Alerta de la CISA (TA13-175A): lanzada en 2016, esta alerta describe por qué es importante cambiar la contraseña predeterminada y brinda acciones de mitigación.
https://www. cisa.gov/uscert/ncas/alerts/TA 13-175A#:~:text=Attackers%20can%20easily%20identify%20and,to%20critical%20and%20important%20systems.

COSTO: **$$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

1.3: ¿Acaso el PWS requiere la MFA siempre que sea posible pero como mínimo para acceder de forma remota a las redes de OT de PWS?

Recomendación: implemente la MFA lo más que se pueda en redes de OT y IT. Como mínimo, se debe implementar la MFA para el acceso remoto a la red de OT.

¿Por qué es importante este control?

La MFA, también llamada autenticación de dos factores, requiere que el personal de PWS y otros usuarios ingresen al menos dos tipos de credenciales independientes cuando inicien sesión en un sistema de PWS. La MFA puede evitar que un atacante que obtenga una contraseña de usuario acceda a redes críticas de PWS. Las credenciales pueden estar basadas en el conocimiento (como una contraseña o un PIN), basadas en activos (como una tarjeta inteligente o un teléfono móvil) o biométricas (como las huellas dactilares). Las credenciales deben provenir de dos categorías diferentes, por lo que ingresar dos contraseñas diferentes no se consideraría una MFA.

Si bien es posible que la MFA no sea necesaria en todos los sistemas, proporciona un mayor nivel de seguridad y debe usarse siempre que sea posible. El acceso de mayor riesgo, como la autenticación de usuarios o proveedores remotos, debe realizarse usando la MFA lo más posible. Muchas aplicaciones de acceso remoto y sistemas de red privada virtual (VPN) ofrecen esta capacidad o se pueden configurar para ofrecerla usando una herramienta de terceros.

Lineamientos adicionales

- Utilice la MFA para verificar la identidad de un usuario siempre que sea posible. Los métodos comunes de la MFA incluyen datos biométricos, tarjetas inteligentes, activos de hardware habilitados para la autenticación rápida en línea (FIDO)/protocolo de cliente a autenticador (CTAP) o códigos de acceso únicos enviados o generados por activos previamente registrados como un teléfono móvil.
- Dentro de las redes de OT, habilite la MFA en todas las cuentas y los sistemas a los que el PWS pueda acceder de forma remota, incluidas las cuentas de proveedores y de mantenimiento, las cuentas de usuario, las estaciones de trabajo de ingeniería y las aplicaciones de HMI.

Consejos de implementación

Revise todas las actividades de acceso remoto, en particular a los sistemas de OT, e identifique si el PWS puede habilitar la MFA en el software utilizado para el acceso. Hay varias aplicaciones que pueden ayudar a habilitar la autenticación de múltiples factores en un PWS. Algunas de los más populares incluyen TeamViewer y Microsoft 365 para Windows. En la sección de recursos a continuación, encontrará los enlaces de la configuración.

Si el PWS no puede usar la MFA (como algunas cuentas de administrador del sistema, raíz o de servicio), esas cuentas deben usar contraseñas que sean únicas para ese sistema y no se debe poder acceder a ellas de forma remota siempre que sea posible.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte la página 132, Identificación y autenticación, para obtener más información sobre la MFA. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Referencia de autenticación de múltiples factores de Microsoft 365: en esta página, se describe cómo configurar los ajustes de autenticación de múltiples factores en las cuentas de Microsoft 365. *https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi- factor-authentication?view=o365-worldwide*

Referencia de autenticación de TeamViewer: en esta página, se describe cómo configurar los ajustes de autenticación de múltiples factores en la plataforma TeamViewer. *https://community.teamviewer.com/English/kb/articles/109255-enable-two-factor-authentication-enforcement-on-company-members*

Seguridad de cuentas: seguridad mínima de la contraseña

COSTO: **$**$$$ IMPACTO: **ALTO** COMPLEJIDAD : **BAJA**

1.4: ¿Acaso el PWS requiere una longitud mínima para las contraseñas?

Recomendación: cuando sea posible, implemente un requisito de longitud mínima para las contraseñas. La implementación puede ser a través de una política o controles administrativos configurados en el sistema.

¿Por qué es importante este control?

El uso de contraseñas cortas en un PWS es un riesgo de seguridad significativo, ya que las contraseñas cumplen un papel vital para evitar que los atacantes accedan a las cuentas de los usuarios. Los atacantes usan programas para adivinar las contraseñas de los usuarios, y una contraseña más larga y compleja les resulta más difícil de descifrar. La gestión completa de las contraseñas incluye determinar la longitud y la complejidad de la contraseña (p. ej., usar letras mayúsculas y minúsculas) y garantizar que los usuarios sigan las prácticas recomendadas sobre la seguridad de las contraseñas (p. ej., no dejar notas adhesivas de recordatorio pegadas en los monitores).

Lineamientos adicionales

- Cree una política o configure controles administrativos que exijan una longitud mínima de la contraseña (se recomiendan 15 caracteres o más) para todos los activos de OT y IT protegidos con contraseña, según sea posible.
- En los casos en que las longitudes mínimas de la contraseña no sean factibles, utilice controles de seguridad de compensación (p. ej., utilizar un inicio de sesión único) y registre todos los intentos de inicio de sesión. Además, si los activos informáticos no admiten contraseñas más largas, priorícelos para actualizarlos o reemplazarlos.
- Utilice contraseñas más largas o frases como contraseña (p. ej., "Iliketoeatapplesandbananas" (megustacomermanzanasybananas).

Consejos de implementación

Si un PWS no tiene actualmente un documento de política que aborde los requisitos de las contraseñas, incluida la longitud mínima y la complejidad, elabore uno y asegúrese de compartirlo con todos los empleados del PWS.

En el caso de los activos de OT y IT basados en Windows, según la versión de Windows, el administrador del sistema puede usar la política de seguridad local para establecer una longitud mínima para las contraseñas. Para acceder a esta función, escriba "Local Security Policy" (Política de seguridad local) en el cuadro de búsqueda del menú de Inicio y haga clic en la aplicación Política de seguridad local. Una vez que se abra el panel del menú, haga clic en Account Policies (Políticas de la cuenta) y luego en Password Policy (Política de contraseñas) para ajustar la longitud de la contraseña.

Si un PWS utiliza un dominio de Microsoft con muchos sistemas y las cuentas de usuario están conectadas a un solo dominio, puede administrar estos ajustes usando los objetos de directiva de grupo (GPO). El administrador del sistema puede configurar la Política de contraseñas en la siguiente ubicación en la consola de administración de políticas de grupo: Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy (Configuración del equipo\Ajustes de Windows\Ajustes de seguridad\Políticas de cuenta\Política de contraseñas). En el enlace de la Referencia de ajustes de la política de contraseñas de Microsoft Windows a continuación, encontrará detalles adicionales.

Para todas las demás contraseñas en activos no basados en Windows, el administrador debe revisar las contraseñas existentes para asegurarse de que cumplan con la política de contraseñas cuando sea posible. Estos activos pueden incluir hardware de red (p. ej., conmutadores de red, puntos de acceso inalámbrico, enrutadores de red); activos de comunicaciones (p. ej., radios); activos de OT (p. ej., PLC y HMI); y aplicaciones de software que utilizan contraseñas para autenticar a los usuarios.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: proporciona un enfoque proactivo y sistémico a fin de desarrollar y poner a disposición un conjunto integral de medidas de protección para todo tipo de plataformas informáticas. Consulte el control AC-1 (página 39) para obtener más información sobre Política y procedimientos de control de acceso. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Lineamientos sobre las contraseñas del NIST: el NIST creó un video breve en el que explica la protección con contraseña y brinda lineamientos sobre la implementación de las mejores prácticas. *https://www.nist.gov/video/password-guidance-nist-0*

Guía de política de contraseñas de control del CIS: el Centro para la Seguridad de Internet (CIS) proporciona una explicación detallada de cómo crear e implementar una política de contraseñas; los detalles sobre la longitud de la contraseña comienzan en la página 7. *https://www.cisecurity.org/insights/white-papers/cis- password-policy-guide*

Consejo de seguridad de la CISA (ST04-002): el Departamento de Seguridad Nacional de EE. UU. ofrece consejos sobre contraseñas efectivas. *https://www.cisa.gov/uscert/ncas/tips/ST04-002*

Referencia de los ajustes de la política de contraseñas de Microsoft Windows: En esta página, se describe cómo configurar los ajustes de la política de contraseñas en los sistemas de Windows.

Seguridad de cuentas: Separación de cuentas de usuario y con privilegios

COSTO: **$**$$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

1.5: ¿Acaso el PWS separa las cuentas de usuario de las que tienen privilegios (p. ej., administrador del sistema)? **Recomendación:** restrinja los privilegios del administrador del sistema para separar las cuentas del usuario solo para tareas administrativas y evalúe los privilegios administrativos periódicamente para asegurarse de que las personas que tienen estos privilegios aún los necesiten.

¿Por qué es importante este control?

El uso indebido de los privilegios administrativos es un método principal para que los atacantes ingresen a una red. En uno de esos métodos, se engaña al usuario de una estación de trabajo que inició sesión como administrador o a un usuario con privilegios para que abra un archivo adjunto de correo electrónico malicioso, descargue y abra un archivo de un sitio web malicioso, o simplemente navegue por un sitio web que tenga contenido de un atacante que puede vulnerar automáticamente los navegadores. Si la víctima inició sesión como administrador, el atacante puede usar este acceso para lanzar un ataque, como implementar ransomware o instalar registradores de pulsaciones de teclas, analizadores de protocolos y software de control remoto para encontrar contraseñas y otros datos confidenciales. Una segunda técnica comúnmente utilizada por los atacantes es un ataque de elevación de privilegios en el que adivinan la contraseña del administrador del sistema. Si un PWS distribuye libre y ampliamente contraseñas administrativas o las configura de manera idéntica a las contraseñas utilizadas en sistemas menos críticos, al atacante le resulta mucho más fácil obtener el control total de un sistema.

Lineamientos adicionales

- En un PWS, debe haber una lista o un inventario actualizados de todas las cuentas del administrador.
- Asegúrese de que todos los usuarios con acceso a cuentas administrativas utilicen una cuenta exclusiva o secundaria para sus actividades administrativas. Esta cuenta solo debe usarse para aquellas actividades administrativas y no para navegar por Internet, correo electrónico o actividades cotidianas similares.
- Limite el acceso a las herramientas de secuencias de comandos (como Microsoft PowerShell y Python) solo a los usuarios administrativos o de desarrollo que necesiten acceder a estas herramientas.
- Configure sistemas para crear una entrada de registro y emitir una alerta cuando el PWS agregue o elimine una cuenta de cualquier grupo que tenga privilegios administrativos. Haga lo mismo para cualquier inicio de sesión fallido en una cuenta administrativa.

Consejos de implementación

Revise todas las cuentas de usuario de OT y IT para determinar cuáles están configuradas actualmente como Usuario estándar o Administrador. En el caso de las cuentas que actualmente estén configuradas como Administrador, revise si ese usuario necesita privilegios de administrador para sus funciones. De lo contrario, el PWS debería asignarle al usuario una cuenta de usuario estándar. Si necesita privilegios de administrador, pero actualmente no tiene una cuenta de usuario estándar para las funciones diarias, el PWS debe crear una cuenta de usuario estándar por separado para ese individuo para uso diario.

El PWS debe restringir el uso de la cuenta de administrador a aquellas personas que necesitan acceso con privilegios y que solo se usen para funciones exclusivas.

En el caso de un PWS que use Windows, hay cinco formas de averiguar qué tipo de cuenta tiene un usuario (consulte los enlaces de Recursos a continuación). Conocer el tipo de cuenta de cada usuario permite al PWS determinar si es necesario cambiar el tipo de cuenta de un usuario a fin de permitir o restringir privilegios adicionales para realizar tareas administrativas.

Un PWS también puede cambiar el nivel de una cuenta en un sistema operativo común: vaya a Settings (Ajustes) > Accounts (Cuentas) > Family & Other Users (Familia y otros usuarios), seleccione la cuenta en cuestión, haga clic en Change Account Type (Cambiar tipo de cuenta) y seleccione Administrator (Administrador) o Standard User (Usuario estándar).

Recursos

- **15 aspectos fundamentales de la seguridad cibernética de WaterISAC:** en la página 15, encontrará más información sobre la separación de cuentas. *https://www.waterisac.org/system/files/articles/15 Cybersecurity Fundamentals %28WaterISAC%29.pdf*
- **Norma del NIST 800-53. Política y procedimientos de control de acceso, AC-1:** en la página 18, encontrará información sobre el control y la gestión de acceso. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*
- **Norma NIST 800-82. Guía para la seguridad del sistema de control industrial (ICS):** En la sección 6.2.1.1, encontrará información adicional sobre el control de acceso basado en roles para los sistemas de control de supervisión y adquisición de datos (SCADA). *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*
- **Windows Central:** identifica cinco formas de saber el tipo de cuenta de los usuarios dentro de una red en Windows. *https://www.windowscentral.com/how-determine-user-account- type-windows-10#determine_windows10_account_type_settings*

Seguridad de cuentas: credenciales únicas

COSTO: **$$**$$ IMPACTO: **MEDIA** COMPLEJIDAD: **MEDIA**

1.6: ¿Acaso el PWS requiere credenciales únicas y separadas para que los usuarios accedan a las redes de OT y de IT?

Recomendación: requiera que un solo usuario tenga dos nombres de usuario y contraseñas diferentes; un conjunto se utilizará para acceder a la red de IT y el otro para acceder a la red de OT. Esto reduce el riesgo de que un atacante pueda moverse entre ambas redes utilizando un solo inicio de sesión.

¿Por qué es importante este control?

El uso de nombres de usuario y contraseñas por separado para los usuarios de las redes de OT y IT es una parte integral de una estrategia de la defensa profunda. Por lo general, si un atacante puede determinar el inicio de sesión de un usuario en una red, utilizará esa misma información para intentar acceder a otras cuentas o redes. Esta técnica puede permitir que un atacante se mueva lateralmente en un entorno operativo de PWS. Además, es posible que no genere ninguna alarma si el monitoreo del sistema no reconoce la actividad como nueva en el entorno operativo y puede hacer que un PWS no detecte el incidente de seguridad. Los delincuentes también pueden usar la función de recuperación de contraseña en una cuenta para acceder a cualquier otra que use la misma dirección de correo electrónico.

Lineamientos adicionales

- Cuando sea factible, nunca permita que varios usuarios compartan un solo inicio de sesión o que un solo usuario use el mismo inicio de sesión para las redes de OT y de IT.

Consejos de implementación

Desarrolle una política que requiera que las personas usen cuentas separadas para OT y IT. Si el PWS tiene un solo dominio de Windows que cubre los sistemas de OT y IT, evalúe dividir ese dominio en dos para evitar que los usuarios compartan cuentas entre los tipos de sistemas. Cuando los usuarios ya tengan cuentas separadas para OT y IT, sugiérales no usar la misma contraseña en estas cuentas.

Los dos sistemas operativos más comunes son Microsoft Windows y Linux. Ambos sistemas permiten que un administrador del sistema administre cuentas y credenciales de cuentas para cada usuario final. Como se mencionó anteriormente, la capacidad de separar las cuentas de los usuarios finales es fundamental en cualquier estrategia de defensa profunda. En los recursos a continuación, encontrará los detalles sobre cómo administrar las cuentas de usuario de cada sistema.

Recursos

Mejora de la seguridad cibernética del sistema de control industrial con estrategias de defensa profundas: en la página 25, encontrará información de administración de cuentas de la red de OT. Nota: La CISA utiliza el término sistema de control industrial (ICS) para referirse a una red de OT.
https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Administración de cuentas de usuario en Windows: proporciona más información sobre cómo administrar cuentas de usuario en Windows. *https://learn.microsoft.com/en-us/windows-server-essentials/manage/manage-user-accounts-in-windows-server-essentials*

Administración de cuentas de usuario en Linux: proporciona más información sobre cómo administrar cuentas de usuario en Linux. *https://www.makeuseof.com/user-management-linux-guide/*

Seguridad de cuentas: revocación de las credenciales de los empleados cesantes

COSTO: **$**$$$ IMPACTO: **MEDIA** COMPLEJIDAD: **BAJA**

1.7: ¿Acaso el PWS deshabilita inmediatamente el acceso a una cuenta o red cuando ya no se requiere debido a que la persona se retiró, cambió de puesto, dejó de trabajar allí u otros factores?
Recomendación: tome todas las medidas necesarias para cancelar el acceso a cuentas o redes ante un cambio en el estado de una persona que hace que el acceso sea innecesario.

¿Por qué es importante este control?

Las cuentas inactivas pueden parecer inofensivas, pero presentan graves riesgos de seguridad cuando un PWS no las desactiva o cuando no tienen límites de caducidad de la contraseña. Los atacantes pueden usar estas cuentas, ya que el PWS posiblemente no se dé cuenta de sus actividades. Además, los empleados que abandonan el PWS aún podrían usar sus credenciales de inicio de sesión para acceder a los recursos de la red, lo que puede ser particularmente riesgoso si el empleado se fue en circunstancias difíciles.

Lineamientos adicionales

- Cancele el acceso a cuentas o redes ante un cambio en el estado de un usuario que hace que el acceso sea innecesario.
- Revoque el acceso a los empleados, los proveedores, los contratistas y los consultores a los que se despidieron y que renunciaron voluntariamente lo más pronto posible.
- Evalúe la necesidad de acceso de los miembros del personal en caso de ascenso u otro cambio de función dentro del PWS y elimine cualquier privilegio de acceso que ya no requieran para su nueva función.
- Establezca un procedimiento de desvinculación con Recursos Humanos, los gerentes de Contratación y el personal de OT y IT. En el procedimiento, se debe incluir un proceso de auditoría para identificar las cuentas que el PWS debe desactivar y eliminar.
- Deshabilite el acceso físico y cibernético de una persona a las instalaciones y a los sistemas de PWS apenas la persona ya no necesite acceder a ellos.

Consejos de implementación

Puede ser útil desarrollar una lista de verificación simple que el PWS pueda usar cuando una persona abandone el PWS o pase a ocupar un nuevo puesto en PWS. En la lista de verificación, se podrían incluir puntos como la devolución de cualquier equipo informático proporcionado por PWS, como computadoras portátiles, tabletas y teléfonos inteligentes, así como la eliminación de las cuentas de usuario de la persona o el cambio de privilegios en las cuentas del usuario según sea necesario.

Recursos

15 aspectos fundamentales de la seguridad cibernética de WaterISAC: en la página 17, se proporciona más información sobre la revocación de credenciales.
https://www.waterisac.org/system/files/articles/15 Cybersecurity Fundamentals %28WaterISAC%29.pdf

COSTO: **$$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

2.1: ¿Acaso el PWS requiere aprobación antes de instalar o implementar un nuevo software?
Recomendación: solo permita a los administradores instalar software nuevo en un activo emitido por el PWS.

¿Por qué es importante este control?

Los usuarios pueden utilizar el software para realizar actividades comerciales normales o con fines maliciosos destinados a dañar el sistema informático o la empresa. Un atacante puede ocultar el software malicioso como un software normal con la intención de engañar a un usuario para que lo instale, al publicitar funciones legítimas sin revelar las funciones maliciosas o al imitar el estilo o la dirección web del portal de descarga de un proveedor de confianza. Un atacante puede incluso comprometer el software de un proveedor legítimo a través de un ataque a la cadena de suministro (p. ej., el ataque a SolarWinds en 2020).

Si un empleado de PWS instala software malicioso de manera intencional o no, el PWS podría quedar expuesto a las vulneraciones, las interrupciones o los daños del sistema. Permitir solo el software aprobado en los activos de PWS, preferentemente que lo instale un administrador, permite que el PWS se asegure de que el software esté libre de código malicioso antes de la instalación.

Lineamientos adicionales

- Establezca controles para las computadoras proporcionadas por PWS y otros activos a fin de restringir el software que los usuarios pueden instalar.
    - Algunos ejemplos son la restricción de privilegios administrativos (es decir, solo ciertas personas designadas pueden instalar software en las computadoras de un PWS, como un administrador del sistema) o solo permitir descargas de software aprobadas.
- Implemente un proceso que requiera aprobación antes de que los usuarios puedan instalar software nuevo o versiones de software.
- Elabore una lista de los riesgos del software permitido por PWS, incluida la especificación de las versiones aprobadas cuando sea técnicamente factible.

Consejos de implementación

Un PWS puede administrar el software disponible para el personal a través de un portal de descarga en cada activo (p. ej., el Centro de Software de Windows) o, más simple, desde una lista de software aprobados. Para instalar un nuevo software, el empleado de PWS debe enviar una solicitud al personal de OT/IT o al administrador del sistema que justifique su necesidad operativa.

Recursos

GAO-22-104746. Respuesta federal a los incidentes de SolarWinds y Microsoft Exchange: consulte la sección Qué encontró la GAO para obtener más información sobre el ataque a la cadena de suministro de SolarWinds en 2020. *https://www.gao.gov/products/gao-22-104746*

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control CM-11 (página 112) para obtener más información sobre el software instalado por el usuario *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Microsoft Learn: guía para el usuario del Centro de software: consulte este recurso para obtener más información sobre cómo planificar y configurar el Centro de Software de Microsoft. *https://learn.microsoft.com/en- us/mem/configmgr/apps/plan-design/plan-for-software-center?source=recommendations*

Seguridad de dispositivos: deshabilitar macros de forma predeterminada

COSTO: **$**$$$ IMPACTO: **MEDIA** COMPLEJIDAD: **BAJA**

2.2: ¿Acaso el PWS deshabilita las macros de Microsoft Office o un código incorporado similar de forma predeterminada en todos los activos?

Recomendación: deshabilite las macros incorporadas y el código ejecutable similar de forma predeterminada en todos los activos.

¿Por qué es importante este control?

Las macros (es decir, el código incorporado) son instrucciones de software que se encuentran en otros archivos, como los documentos de Microsoft Office Word o las hojas de cálculo de Excel. Tener estas macros en un archivo puede ser útil para automatizar tareas repetitivas o actualizar datos de fuentes en línea. Sin embargo, los atacantes suelen utilizar estas macros para ejecutar código malicioso, descargar malware y virus o robar datos.

Un atacante puede entregar un archivo con macros maliciosas a un empleado de PWS como un archivo adjunto de un correo electrónico de phishing. Si el empleado descarga el archivo, la macro dentro de este puede provocar que el sistema informático del PWS quede expuesto a vulneraciones, interrupciones o daños. Si se deshabilitan las macros de forma predeterminada, un PWS puede reducir el riesgo del código ejecutable.

Lineamientos adicionales

• Cuando sea necesario para fines importantes, un PWS puede habilitar las macros en determinados activos.

Consejos de implementación

Si bien un usuario puede cambiar este ajuste localmente en activos individuales, el PWS debe implementarla en toda la organización a través de una política aplicada por el sistema.

El PWS debe tener una política para que los usuarios autorizados envíen una solicitud para habilitar las macros. Esta solicitud debe justificar la necesidad operativa de habilitar las macros para que el personal de OT/IT pertinente o el administrador del sistema puedan tomar la decisión de permitir o rechazar la solicitud en función del potencial riesgo para las operaciones del PWS.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control SC-18 (página 311) para obtener más información sobre la gestión de macros, denominado Código móvil. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Microsoft Learn. Bloqueo de la ejecución de las macros en archivos de Office provenientes de Internet: consulte este recurso para obtener información sobre cómo configurar Windows para bloquear las macros de Internet.
https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked#block-macros-from-running-in-office-files-from-the-internet

COSTO: **$$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

2.3: ¿Acaso el PWS mantiene un inventario actualizado de todos los activos de red de OT y IT?
Recomendación: haga una revisión (no menos de una vez al mes) y un mantenimiento con regularidad de la lista de todos los activos de OT y IT con una dirección IP. Esto incluye equipos heredados (es decir, más antiguos) y de terceros.

¿Por qué es importante este control?

Un PWS no puede proteger ni asegurar lo que no sabe que tiene. Tener un inventario preciso de los activos tecnológicos de OT (p. ej., SCADA, PLC, HMI) y IT (p. ej., computadoras de oficina, conmutadores de red, servidores) es una parte fundamental de la seguridad cibernética del PWS. Una vez que el PWS sepa qué activos tiene, puede realizar las mejoras de seguridad cibernética necesarias en las redes de OT y IT.

Un PWS necesita comprender qué activos se encuentran en sus sistemas de SCADA, de comunicaciones y comerciales. Tener un inventario preciso permitirá que el PWS conozca mejor sus activos, lo ayudará a encontrar las vulnerabilidades en estos y ayudará a los PWS a responder con más facilidad a los ataques cibernéticos.

Lineamientos adicionales

- Sobre la base de la revisión, actualice los registros obsoletos de los activos conocidos, agregue activos previamente desconocidos al inventario y elimine los activos de la lista que el PWS ya no use.
- Asegúrese de que en la lista se identifiquen los activos físicos y también incluya los detalles de estos, lo que incluye cómo están conectados, qué datos comparten y quién en el PWS (o qué proveedor) trabaja con el activo.

Consejos de implementación

Hay varios métodos para identificar y hacer un inventario de los activos, y el mejor enfoque probablemente sea una combinación de inspección física, exploración pasiva, exploración activa y análisis de configuración (establecimiento). Es importante tener esta información a fin de prepararse para un ataque cibernético o responder a él; sin embargo, también es valiosa para un atacante, por lo que debe protegerse como corresponde.

Identificar y elaborar un inventario de los activos es un primer paso importante que debe tomar un PWS para conocer sus activos. Los PWS deben saber qué activos tienen, cómo están configurados (consulte la hoja informativa 2.5) y cómo están conectados esos activos (consulte la hoja informativa 7.4).

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control CM-8 (página 107) para obtener más información sobre el Inventario de componentes del sistema. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Publicación en el blog de seguridad del sistema de control industrial (ICS) del Instituto SANS: "Know Thyself
Better than the Adversary - ICS Asset Identification and Tracking" (Conózcase más a usted que el adversario: identificación y seguimiento de activos del ICS): proporciona información sobre identificación y seguimiento de activos. *https://www.sans.org/blog/know-thyself- better-than-the-adversary-ics-asset-identification-and-tracking/*

15 aspectos fundamentales de la seguridad cibernética de WaterISAC: consulte la sección en la página 7, Realizar inventarios de activos para obtener información adicional. *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

Seguridad de dispositivos: prohibición de la conexión de activos no autorizados

COSTO: **$$$**$ IMPACTO: **ALTO** COMPLEJIDAD: **ALTO**

2.4: ¿Acaso el PWS prohíbe la conexión de hardware no autorizado (p. ej., dispositivos USB, unidades extraíbles, computadoras portátiles que llevan otras personas) a activos de OT y IT?

Recomendación: cuando sea factible, elimine, deshabilite o asegure los puertos físicos (p. ej., los puertos USB en una computadora portátil) para evitar que se conecten activos no autorizados.

¿Por qué es importante este control?

Aunque los ataques cibernéticos provenientes de Internet reciben la mayor parte de la atención, incluso si un PWS no conecta una red a Internet (por ejemplo, un espacio de aire), aún podría ser vulnerable a los ataques de conexiones directas. Por ejemplo, si un empleado o proveedor utiliza una unidad de Bus Universal en Serie (USB) o una computadora portátil de terceros fuera del PWS y luego la conecta a la red del PWS, puede introducir malware en los sistemas de IT o de OT del PWS (ya sea intencionalmente o no).

La conexión de un activo USB malicioso a la red de PWS puede provocar vulneraciones, interrupciones o daños en el sistema. El ejemplo más conocido de un atacante que usa un USB para dañar una planta industrial es Stuxnet, el primer malware conocido públicamente diseñado para atacar los sistemas de OT. Solo permitir que los activos autorizados se conecten a las redes de PWS ayuda a evitar que los atacantes ingresen o roben datos de esas redes.

Lineamientos adicionales

- Deshabilite las funciones de ejecución automática que otorgan acceso automático a las unidades extraíbles (p. ej., unidades USB) cuando la conecte a una computadora.
- Permita el acceso a los puertos de conexión física en las computadoras solo a través de excepciones aprobadas.

Consejos de implementación

Los PWS pueden detener el uso de activos no autorizados mediante el uso de jaulas físicas para cubrir los puertos de la computadora, a través de políticas administrativas (menos efectivas) o al deshabilitar los permisos técnicos usando una política en toda la organización dentro de Microsoft Windows. Si un PWS permite a los usuarios conectar activos externos a sus sistemas, debe verificarlos en busca de malware antes de conectarlos. Los PWS generalmente pueden configurar el software antivirus para escanear automáticamente las unidades externas como las USB cuando un usuario las inserta.

Si es necesario, establezca un proceso administrativo mediante el cual un usuario pueda solicitar una excepción al uso de un activo externo al justificar la necesidad operativa. El personal pertinente de OT/IT o el administrador del sistema deberá sopesar la necesidad operativa frente al posible riesgo de seguridad para los sistemas informáticos del PWS.

Recursos

MITRE ATT&CK. Stuxnet: consulte Replicación a través de medios extraíbles para obtener más información sobre la propagación de Stuxnet. *https://attack.mitre.org/software/S0603/*

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control MP-7 (página 176) y SC-41 (página 326) para obtener más información sobre el Uso de medios y el Acceso a dispositivos de E/S y a puertos. *https://csrc.nist.gov/publications/detail/sp/800- 53/rev-5/final*

Microsoft Learn. Habilitación y deshabilitación de la ejecución automática: consulte la sección sobre Uso del registro para deshabilitar la ejecución automática a fin de obtener más información. *https://learn.microsoft.com/en- us/windows/win32/shell/autoplay-reg#using-the-registry-to-disable-autorun*

COSTO: **$$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

2.5: ¿Acaso el PWS mantiene la documentación actualizada que detalla la instalación y los ajustes (es decir, la configuración) de los activos críticos de OT y IT?

Recomendación: conserve la documentación precisa de la configuración original y actual de los activos de OT y IT, incluida la versión de software y de firmware.

¿Por qué es importante este control?

Si bien un PWS puede conocer los activos físicos que existen en sus redes informáticas al realizar un inventario de activos (consulte la hoja informativa 2.3), también es importante comprender la configuración (es decir, los ajustes) de sus activos. Los atacantes a menudo aprovechan las vulnerabilidades (es decir, las debilidades) que solo existen en ciertas versiones o configuraciones del software y el firmware utilizados para controlar los activos. Por lo tanto, un PWS debe conocer las configuraciones de sus activos para saber si una vulnerabilidad recién encontrada podría usarse en un ataque a la red.

Además, si un atacante cambia la configuración de los activos, borra los ajustes o desactiva los activos, la documentación de configuración bien mantenida permitirá que el PWS detecte los cambios con más facilidad, restablezca los ajustes adecuados y mantenga o restaure las operaciones.

Lineamientos adicionales

- Revise y actualice la documentación de la configuración periódicamente.

Consejos de implementación

Para documentar completamente las configuraciones de los activos, incluya los siguientes detalles, según corresponda: propietario (p. ej., Departamento de Ingeniería), ubicación física y de la red, proveedor, tipo de activo, modelo, nombre del activo, versiones de firmware o de software, niveles de parches, configuraciones de activos, servicios activos (es decir, procesos automatizados), protocolos de comunicación, direcciones de red (p. ej., IP y MAC), valor de los activos e importancia crítica para las operaciones de PWS.

Para ser eficiente, un PWS puede realizar una revisión de la configuración de sus activos al mismo tiempo que el proceso de inventario de activos detallado en la hoja informativa 2.3 y el estudio de la red que figura en la hoja informativa 7.4. La información de la configuración es importante para prepararse para un ataque cibernético o responder a él; sin embargo, también es valiosa para un atacante, por lo que el PWS debería protegerla como corresponde.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte la familia de controles CM-1 (página 96) y el control CM-6 (página 103) para obtener más información sobre Gestión de la configuración y Parámetros de los ajustes.
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

COSTO: **$$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

3.1: ¿Acaso el PWS recopila los registros de seguridad (p. ej., acceso al sistema y a la red, detección de malware) para usarlos tanto en la detección como en la investigación de incidentes?

Recomendación: recopile y almacene registros o datos de tráfico de red para poder detectar ataques cibernéticos e investigar actividades sospechosas.

¿Por qué es importante este control?

El registro es la recopilación de datos sobre los sucesos que tienen lugar en los sistemas de OT o IT de un PWS. Al responder a un ataque cibernético, tener registros detallados ayudará al PWS y a otros investigadores a determinar cómo y cuándo un atacante pudo ingresar en sus sistemas, a qué áreas accedió y si filtró datos confidenciales. Las revisiones periódicas de estos registros también pueden permitirle al PWS detectar a un atacante antes de que pueda afectar los sistemas.

Lineamientos adicionales

- Verifique los registros con regularidad tanto para verificar que estén completos como para asegurarse de que se pueda encontrar toda la información necesaria en caso de un ataque cibernético.
- Si una fuente de registro (p. ej., el registro de eventos de Windows) no está activa, notifique al administrador del sistema o a la persona responsable de la seguridad del sistema.
- Si los registros no están disponibles para ciertos activos de OT, recopile información sobre el tráfico de la red y las comunicaciones hacia estos activos y desde ellos.

Consejos de implementación

Las fuentes de registros incluyen, entre otras, inicios de sesión en la red y registros de servidores, activos de usuarios finales (p. ej., computadoras de escritorio y portátiles), equipos de red (p. ej., enrutadores y conmutadores), aplicaciones/programas, sistemas de detección de intrusiones/sistemas de protección contra intrusiones (IDS/IPS), cortafuegos, software antivirus, herramientas de prevención de pérdida de datos (DLP) y redes privadas virtuales (VPN).

Si es posible, los PWS deben capturar, revisar y almacenar de forma segura los registros de todas estas fuentes para referencia futura en caso de un ataque cibernético. Como mínimo, los PWS deben habilitar el registro en servidores críticos, cortafuegos y herramientas de acceso remoto como las VPN. En los manuales de configuración de cualquier cortafuegos o herramienta de acceso remoto, debería encontrar instrucciones sobre cómo configurar y habilitar el registro para estos activos específicos.

En el caso de los sistemas basados en Windows, la aplicación Visor de eventos de Windows le brinda al PWS la capacidad de revisar manualmente los registros de seguridad de un activo individual. Para ver un registro de seguridad de ejemplo en Windows, abra la aplicación Visor de eventos. En el árbol de la consola, expanda Windows Logs (Registros de Windows) y, luego, haga clic en Security (Seguridad). En el panel de resultados, se mencionan los eventos de seguridad individuales. Para ver más detalles sobre un evento específico, haga clic en él en el panel de resultados. El PWS puede recopilar eventos de Windows de servidores y puntos de conexión (p. ej., computadoras de escritorio y portátiles) en un servidor central para un análisis manual más eficiente utilizando el Recopilador de eventos de Windows.

Si bien el método es una mejora con respecto a la revisión de registros totalmente manual, no incluirá registros de activos y aplicaciones que no sean de Windows, lo que proporciona un panorama incompleto de las operaciones del PWS.

Para abordar este problema, el PWS puede utilizar software de incorporación de registros y sistemas de gestión de eventos de información de seguridad (SIEM) para recopilar registros de forma centralizada de prácticamente todas las fuentes, simplificar la revisión de los registros y detectar los eventos de interés. Además de tener todos los registros en un solo lugar, estas herramientas también pueden automatizar muchos pasos del análisis de registros, lo que hace que el equipo de seguridad de PWS sea más eficaz, además de que permiten ahorrar tiempo en el proceso.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control AU-2 (página 66) para obtener más información sobre Registro de eventos. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

15 aspectos fundamentales de la seguridad cibernética de WaterISAC: consulte la página 31 para obtener más información sobre Registro y auditoría. *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

Microsoft Learn. Recopilador de eventos de Windows: consulte este recurso para obtener más información sobre cómo configurar el Recopilador de eventos de Windows.

Seguridad de los datos: almacenamiento seguro de los registros

COSTO: **$$$**$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

3.2: ¿Acaso el PWS protege los registros de seguridad contra el acceso no autorizado y la manipulación?
Recomendación: almacene los registros de seguridad en un sistema central o en una base de datos a la que solo puedan acceder los usuarios autorizados y autenticados.

¿Por qué es importante este control?

Una vez que el PWS recopile los registros de seguridad, debe almacenarlos y protegerlos. Este paso es importante porque, si un atacante compromete un sistema, puede modificar o eliminar los registros para destruir la evidencia y cubrir sus huellas.

Sin datos de registro confiables para rastrear lo que hace un atacante en un sistema informático de PWS, tanto detectar como responder a un ataque cibernético se vuelven mucho más difíciles. El administrador del sistema no sabrá a dónde fue el atacante, qué hizo o cuándo lo hizo. Este paso ayuda a garantizar que el PWS proteja sus registros de seguridad contra el acceso no autorizado y la manipulación.

Lineamientos adicionales

- Almacene los registros durante un determinado período que tenga en cuenta la política de PWS, las normas estatales (si las hubiere) y el riesgo cibernético. Un período habitual de conservación de registros es de seis meses.
- Asegúrese de que los registros de seguridad sean parte de los procedimientos estándares de copia de seguridad del PWS para que este pueda revisar los registros, incluso si la fuente ya no está disponible.

Consejos de implementación

Se pueden almacenar los registros en un sistema o en una base de datos centrales utilizando los sistemas de gestión de eventos e información de seguridad (SIEM), que se abordan más detalladamente en la hoja informativa 3.1. Además de facilitar la recopilación y el análisis de registros, las herramientas de SIEM también le permiten al administrador del sistema configurar los permisos de acceso por usuario, lo que se conoce como control de acceso basado en roles (RBAC). Cuando almacene los registros en una ubicación central con una herramienta de SIEM o sin ella, asegúrese de que cada usuario tenga una cuenta individual para acceder al almacenamiento de registros (es decir, herramienta de SIEM, base de datos de registros o servidor de registros).

Independientemente de cómo el PWS guarde los registros, debe hacer una copia de seguridad en una unidad de almacenamiento secundaria de forma regular. Una frecuencia común es a diario. Los requisitos y restricciones reglamentarios, operativos y tecnológicos suelen determinar durante cuánto tiempo se guardarán los registros; sin embargo, es común conservarlos durante seis meses. Por lo general, es mejor guardar un registro durante un período más largo que corto, ya que los encuestados tendrán más evidencia que revisar al investigar un posible ciberataque.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte la familia de controles AU y AU-9 (página 74) para obtener más información sobre Auditoría y responsabilidad y Protección de la información de auditoría.
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

15 aspectos fundamentales de la seguridad cibernética de WaterISAC: consulte la página 31 para obtener más información sobre Registro y auditoría. *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

Microsoft Learn. Configuración o personalización de la copia de seguridad del servidor: consulte este recurso para obtener más información sobre cómo configurar copias de seguridad para unidades de almacenamiento de registros. *https://learn.microsoft.com/en-us/windows-server-essentials/manage/set-up-or-customize- server-backup*

COSTO: **$$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

3.3: ¿Acaso el PWS utiliza un cifrado eficaz para mantener la confidencialidad de los datos en tránsito?
Recomendación: cuando envíe datos e información, utilice los estándares de cifrado de seguridad de la capa de transporte (TLS) o de la capa de sockets seguros (SSL).

¿Por qué es importante este control?

El cifrado es el proceso mediante el cual las computadoras convierten información (p. ej., archivos, tráfico de red) de texto simple que las personas pueden leer en un mensaje codificado que no pueden leer. Es un paso importante, ya que los atacantes a menudo intentarán interceptar mensajes para alterar los comandos de los activos de OT y robar contraseñas u otra información confidencial.

Si se usa un cifrado seguro al enviar información, incluso si los atacantes logran interceptar un mensaje, no podrán usar la información ya que no la podrán leer. Este paso ayuda a mantener la privacidad (es decir, el secreto) de la información confidencial y la integridad (es decir, la precisión) de la información de la OT y la IT.

Lineamientos adicionales

- Para los sistemas informáticos de la OT, como SCADA, utilice el cifrado para las comunicaciones con activos remotos o externos.
- Actualice cualquier software de cifrado de datos inseguro u obsoleto.

Consejos de implementación

TLS y SSL son los protocolos de cifrado más comunes que usan los sistemas para enviar información y datos, y los PWS pueden configurar activos como computadoras de escritorio y servidores para enviar y recibir mensajes cifrados usando uno de estos protocolos. El estándar TLS es una alternativa más nueva y segura que el SSL y, en general, es el estándar de cifrado que se prefiere si es factible. Un PWS debe realizar una revisión del protocolo de cifrado actual que utiliza, comparar este protocolo con los estándares actuales y desarrollar un plan de mejora si es necesario y factible desde el punto de vista operativo.

Los ajustes de configuración para el cifrado pueden estar disponibles para una variedad de comunicaciones, incluido el software de acceso remoto, el software HMI basado en la web, las comunicaciones inalámbricas (p. ej., wifi) y las comunicaciones por radio. Un PWS debe cifrar y proteger con contraseña las comunicaciones inalámbricas y evitar las redes wifi abiertas (es decir, sin contraseña). Es probable que las redes privadas virtuales (VPN) para acceder de manera remota a los sistemas de los PWS y los servicios en la nube para el almacenamiento remoto y el alojamiento de aplicaciones ofrezcan esta función de manera predeterminada.

Dentro de Windows, el PWS puede habilitar el estándar TLS a través del administrador de configuración. Si implementa TLS a través del Administrador de configuración de Windows, asegúrese de comenzar con los clientes/puntos finales (computadoras de escritorio y portátiles). Si comienza la implementación a nivel del servidor, puede cortar la comunicación con los activos del cliente.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: Consulte el control SC-8 (página 304) para obtener más información sobre Confidencialidad e integridad de la transmisión.
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Guía de infraestructura básica de Microsoft: consulte los siguientes enlaces para obtener instrucciones sobre cómo habilitar TLS 1.2 en clientes (p. ej., computadoras de escritorio y portátiles) y servidores a través del Administrador de configuración de Windows.
https://learn.microsoft.com/en-us/mem/configmgr/core/plan- design/security/enable-tls-1-2-client; https://learn.microsoft.com/en- us/mem/configmgr/core/plan-design/security/enable-tls-1-2

COSTO: **$$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

3.4: ¿Acaso el PWS utiliza un cifrado para mantener la privacidad de los datos confidenciales almacenados?
Recomendación: no almacene datos confidenciales, incluidas las credenciales (es decir, nombres de usuario y contraseñas) en texto sin formato.

¿Por qué es importante este control?

Consulte la hoja informativa 3.3 para conocer la importancia del cifrado general.

Este control es importante, ya que los atacantes a menudo intentan acceder a los sistemas informáticos y las bases de datos para robar información confidencial e "inspeccionar" la red para un ataque futuro. Además, muchos cibersecuestros de datos también incluyen intentos de extorsión en los que el atacante roba los datos confidenciales de un PWS y amenaza con exponerlos en Internet si no se paga una cantidad. Si el PWS cifra los datos, el atacante no podrá usarlos si logra robarlos, ya que serán ilegibles.

Lineamientos adicionales

- Solo permita el acceso a usuarios autorizados.
- Actualice cualquier software de cifrado de datos inseguro u obsoleto.

Consejos de implementación

Un PWS puede cifrar los datos almacenados usando BitLocker para el cifrado de unidades de servidores y clientes (computadoras de escritorio y portátiles), así como con el cifrado de datos transparente (TDE) para archivos de bases de datos. Un PWS puede cifrar y proteger con contraseña archivos confidenciales individuales en Windows haciendo clic con el botón derecho en un archivo y seleccionando Properties (Propiedades) -> Advanced (Avanzado) -> Encrypt contents to secure data (Cifrar contenido para proteger datos). Es probable que los servicios en la nube para almacenamiento remoto y alojamiento de aplicaciones ofrezcan esta función de manera predeterminada.

Para almacenar y utilizar las credenciales de forma segura, un PWS puede utilizar un software de gestión de contraseñas (p. ej., LastPass, 1Password) u otro método de administración de cuentas. El software de gestión de contraseñas almacena de forma segura las credenciales, reduce la dificultad de recordar contraseñas y simplifica el uso de contraseñas complejas.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control SC-13 (página 308) y SC-28 (página 317) para obtener más información sobre Protección criptográfica y Protección de información en reposo.
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Guía de infraestructura básica de Microsoft: consulte los siguientes enlaces para obtener instrucciones sobre cómo cifrar los datos almacenados mediante el cifrado de unidades de BitLocker, el cifrado de datos transparente (TDE) para bases de datos y el cifrado de archivos individuales.

https://learn.microsoft.com/en- us/dynamics365/business-central/dev-itpro/security/transparent-data-encryption;

https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview;

https://support.microsoft.com/en-us/windows/how-to-encrypt-a-file-1131805c-47b8-2e3e-a705-807e13c10da7

COSTO: **$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

4.1: ¿Acaso el PWS tiene un rol/puesto/cargo designado que sea responsable de la planificación, la dotación de recursos y la ejecución de las actividades de seguridad cibernética dentro de sí mismo?

Recomendación: identifique una función, un puesto o un cargo responsable de la seguridad cibernética dentro del PWS. Quien lo desempeñe estará a cargo de todas las actividades de seguridad cibernética de PWS.

¿Por qué es importante este control?

Para prepararse y responder a las amenazas de seguridad cibernética de manera eficaz en todo el PWS, es esencial crear una estrategia vertical, que empiece con la asignación de un líder de seguridad cibernética general. El PWS puede asociar la responsabilidad del líder con un puesto de trabajo actual. La persona que ocupe el puesto de liderazgo debe ser responsable de la planificación, la dotación de recursos y la supervisión de la ejecución de las actividades de seguridad cibernética. El líder de seguridad cibernética puede realizar actividades tales como administrar operaciones de seguridad cibernética a nivel superior, brindar capacitación de concientización a los empleados, planificar ejercicios (p. ej., ejercicios de simulación), solicitar y asegurar recursos presupuestarios para actividades de seguridad cibernética, como soporte de proveedores, e informar a la junta o área administrativa sobre las actividades de seguridad cibernética.

Lineamientos adicionales

- Seleccione un puesto dentro del PWS para el rol/puesto/cargo designado como responsable de la seguridad cibernética general. Si es posible, la persona que desempeñe esta función no debe ser también el administrador del sistema. Esta persona debe ser un empleado del PWS, y no un proveedor o contratista, para que el PWS pueda responsabilizarlo por las funciones que realiza.
- Establezca tareas y deberes claros para el líder de seguridad cibernética y regístrelos, como agregándolos a una descripción de puesto existente. Incluya diagramas y fotografías cuando sea necesario.
- Identifique a cualquier miembro del personal esencial que deba ayudar al líder de seguridad cibernética.

Consejos de implementación

La persona responsable como líder general de seguridad cibernética no necesita ser un experto cibernético; sin embargo, sería útil que tuviera cierto conocimiento de cómo funcionan los sistemas de OT y IT del PWS.

Asegúrese de que el líder de seguridad cibernética tenga suficientes oportunidades de capacitación para desempeñar su función de manera eficaz. Incluya las funciones y las responsabilidades del individuo como líder de seguridad cibernética en sus revisiones de desempeño.

Recursos

15 aspectos fundamentales de la seguridad cibernética de WaterISAC: La página 25 brinda información sobre cómo crear una cultura de seguridad cibernética en un PWS, incluida la participación de la administración y la junta.
https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf

Marco de referencia de la fuerza laboral para la seguridad cibernética de la NICCS (marco NICE): este recurso ayuda a los empleadores a desarrollar su fuerza laboral para la seguridad cibernética. Consulte el módulo Gestión de seguridad cibernética. *https://niccs.cisa.gov/workforce-development/nice-framework/specialty- areas/cybersecurity-management*

Cursos de herramientas cibernéticas básicas: este conjunto de herramientas presenta un grupo de módulos diseñados para dividir los fundamentos cibernéticos de la CISA en pasos manejables para un líder de seguridad cibernética.*https://www.cisa.gov/publication/cyber-essentials-toolkits*

COSTO: **$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

4.2: ¿Acaso el PWS tiene un rol/puesto/cargo designado que sea responsable de la planificación, la dotación de recursos y la ejecución de las actividades de seguridad cibernética específicas de la OT?

Recomendación: identifique una función, un puesto o un cargo del PWS responsable de garantizar la planificación, la obtención de recursos y la ejecución de actividades de seguridad cibernética específicas de OT.

¿Por qué es importante este control?

Además de un líder de seguridad cibernética general (consulte la hoja informativa 4.1), los PWS deben asignar un rol/puesto/cargo que se asigne como responsable de las actividades de seguridad cibernética específicas de la OT, debido a sus complejidades. La persona que desempeñe este rol, puesto o cargo de líder de seguridad cibernética de la OT debe poder supervisar y tener autoridad sobre toda la seguridad cibernética específica de la OT y ser responsable de la planificación, la dotación de recursos y la ejecución de todas las actividades de seguridad cibernética específicas de la OT.

Lineamientos adicionales

- Seleccione un puesto dentro del PWS para el rol, puesto o cargo designado como responsable de la seguridad cibernética de la OT. Este líder de seguridad cibernética de la OT podría desempeñar el mismo rol, puesto o cargo mencionado en el punto 4.1, un rol, puesto o cargo distinto en el PWS, un rol, puesto o cargo a nivel municipal o del condado o un rol/, puesto o cargo que supervise un proveedor de OT encargado de dar servicios de seguridad cibernética. El líder de seguridad cibernética de OT puede ser diferente al administrador del sistema. El líder de seguridad cibernética de la OT podría desempeñar el mismo rol, puesto o cargo responsable de las operaciones generales de la OT.
- Establezca y registre tareas claras para el líder de seguridad cibernética de la OT, como agregándolas a la descripción de un puesto existente. Incluya diagramas y fotografías cuando sea necesario.
- Identifique a cualquier miembro del personal esencial que deba ayudar al líder de seguridad cibernética de la OT.

Consejos de implementación

El empleado del PWS responsable como líder de seguridad cibernética de la OT debe tener un buen conocimiento práctico de cómo el PWS configura, usa y mantiene sus sistemas de OT. Por ejemplo, el PWS podría nombrar a un empleado que usa la OT como parte de sus deberes regulares en su rol, puesto o cargo.

Si el líder de seguridad cibernética de la OT realizará completamente sus funciones sin ayuda externa, asegúrese de que el empleado del PWS que cumpla esta función tenga suficientes oportunidades de capacitación para llevar a cabo sus responsabilidades de manera eficaz. Incluya en las revisiones de desempeño las responsabilidades del líder de seguridad cibernética de la OT. Si un proveedor se desempeñará como líder de seguridad cibernética de la OT, el PWS debe incluir un lenguaje a tal efecto en el acuerdo o contrato del nivel de servicio.

Recursos

Seguridad cibernética del ICS para el nivel C del Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC): proporciona ejemplos de seis preguntas de supervisión de riesgos de seguridad cibernética que un líder de seguridad cibernética de OT debe plantearse sobre el entorno de su organización,

e incluye servicios y pasos de acción prácticos específicos para la infraestructura crítica. *https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_ICS_Cybersecurity C-Level S508C.pdf*

Marco de referencia de la fuerza laboral para la seguridad cibernética de la NICCS (marco NICE): este recurso ayuda a los empleadores a desarrollar su fuerza laboral para la seguridad cibernética. Consulte el módulo Gestión de seguridad cibernética. *https://niccs.cisa.gov/workforce-development/nice-framework/specialty- areas/cybersecurity-management*

COSTO: **$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

4.3: ¿Acaso el PWS brinda, por lo menos, capacitaciones anuales para todo el personal del PWS que cubran los conceptos básicos de seguridad cibernética?

Recomendación: lleve a cabo una capacitación básica anual en seguridad cibernética para todo el personal de PWS.

¿Por qué es importante este control?

Para ayudar a crear y mantener una cultura de seguridad cibernética, un PWS debe brindar capacitación básica y periódica sobre seguridad cibernética a todo el personal. Si bien la seguridad cibernética cubre muchas áreas, hay ciertos conceptos básicos de seguridad que el PWS debe enfatizar regularmente para desarrollar una conciencia general y promover mejores prácticas cibernéticas. Cuando los PWS capacitan al personal con regularidad, es más probable que dicho personal identifique y responda rápidamente ante un posible incidente cibernético o que evite que este ocurra del todo. La capacitación regular es fundamental ya que las amenazas de seguridad cibernética evolucionan constantemente.

Lineamientos adicionales

- Establezca un cronograma a fin de realizar capacitaciones periódicas para todo el personal del PWS que cubra los conceptos básicos de seguridad cibernética. La capacitación debe darse una vez al año, como mínimo.
- Establezca una política que requiera que los nuevos empleados reciban capacitación inicial en seguridad cibernética dentro de los 10 días posteriores a su incorporación. La capacitación debe considerar el rol del nuevo empleado y cubrir temas básicos de seguridad.

Consejos de implementación

Desarrolle una agenda para la capacitación que cubra los conceptos básicos de seguridad cibernética, como phishing, riesgo de los correos electrónicos comerciales, seguridad de contraseñas, últimas tendencias y amenazas en ingeniería social y las mejores prácticas de higiene cibernética. La ingeniería social es una forma común de aprovecharse de las personas a través de las redes sociales (p. ej., Facebook) y la interacción humana (p. ej., el correo electrónico) para obtener acceso e información confidencial. Utilice conceptos de capacitación que sean familiares para el personal del PWS, incluidos ejemplos reales basados en los equipos y sistemas que el PWS usa. Por ejemplo, si el PWS entrega un teléfono inteligente al empleado, incluya capacitación específica relacionada con la seguridad de este dispositivo. Dado que probablemente todo el personal reciba un correo electrónico, la capacitación siempre debe incluir las mejores prácticas de seguridad cibernética para revisar y abrir correos electrónicos.

Desarrolle los materiales de capacitación para que sean fáciles de seguir y para que el personal pueda consultarlos más adelante. Actualice las presentaciones de PowerPoint, los módulos de aprendizaje en línea y los folletos para cada capacitación. Comparta enlaces de recursos adicionales donde el personal del PWS pueda obtener más información sobre los temas de seguridad cibernética. Para que la seguridad cibernética se mantenga relevante y actualizada, considere agregar un segmento corto de seguridad cibernética en las reuniones y sesiones informativas del personal del PWS donde se comparta un consejo rápido o información relacionada con la seguridad cibernética.

El personal que suele ser el objetivo de los ataques, como ejecutivos, asistentes ejecutivos, ingenieros, personal de SCADA, personal de IT, operadores y personal de Recursos Humanos y finanzas, debe recibir

una capacitación más especializada. Existen muchas opciones de capacitación gratuitas disponibles en línea y presencialmente, incluso de la CISA y la Iniciativa Nacional para Carreras y Estudios en Ciberseguridad (NICCS) (consulte los siguientes recursos).

Recursos

15 aspectos fundamentales de la seguridad cibernética de WaterISAC: la página 25 proporciona información para crear una cultura de seguridad cibernética en un PWS, incluida la capacitación de concientización sobre seguridad cibernética para todo el personal del PWS.
https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf

Norma 800-16 y 800-50 del NIST. Desarrollo de un programa de capacitación y concientización sobre la seguridad de la tecnología de la información: Brinda orientación para crear un programa de capacitación y concientización sobre la seguridad de la IT.
https://csrc.nist.gov/publications/detail/sp/800-50/final;
https://csrc.nist.gov/publications/detail/sp/800-16/final

Norma NIST 800-82. Guía para la seguridad de los sistemas de control industrial: la sección 6.2.2 de la página 6-13 proporciona una guía de capacitación del ICS.
https://csrc.nist.gov/publications/detail/sp/800- 82/rev-2/final

Capacitación de la CISA: brinda capacitación en línea sin costo sobre una variedad de temas de seguridad cibernética. *https://www.cisa.gov/cybersecurity-training-exercises*

Portal de aprendizaje virtual de la CISA: brinda capacitación en línea sin costo sobre una variedad de temas de seguridad cibernética. *https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA#need*

Capacitación en seguridad cibernética de Federal Virtual Training Environment (FedVTE) de la NICCS: brinda capacitación sobre seguridad cibernética en línea sin costo para empleados gubernamentales estatales, locales, tribales y territoriales. *https://niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte*

Stop Ransomware.gov: es el sitio único oficial del Gobierno de EE. UU. para obtener recursos que abordan el ransomware de manera más eficaz. *https://www.cisa.gov/stopransomware*

COSTO: **$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

4.4: ¿Acaso el PWS ofrece capacitación sobre seguridad cibernética específica de la OT al menos una vez al año al personal que usa la OT como parte de sus funciones regulares?

Recomendación: brinde capacitación especializada en seguridad cibernética centrada en la OT a todo el personal que utiliza activos de OT.

¿Por qué es importante este control?

La hoja informativa 4.3 presenta la importancia de las capacitaciones regulares sobre seguridad cibernética básica para todo el personal. Además, el personal que da mantenimiento o protección a la OT como parte de sus funciones regulares debe recibir capacitación específica en seguridad cibernética de OT al menos una vez al año.

Lineamientos adicionales

- Identifique al personal del PWS que debe recibir capacitación en seguridad cibernética más especializada y centrada en la OT. Como mínimo, los PWS deben brindar esta capacitación especializada al personal que utiliza los activos de OT como parte de sus funciones habituales.

Consejos de implementación

El proveedor de OT designado por el PWS puede ser capaz de realizar la capacitación en seguridad cibernética centrada en OT para el PWS.

En lugar de una gran capacitación que cubra muchos temas, un PWS debe realizar múltiples capacitaciones programadas periódicamente a lo largo del año para ayudar a dividir los temas en sesiones breves y digeribles.

Desarrolle la agenda y los materiales de capacitación para que sean fáciles de seguir y para que el personal pueda consultarlos más adelante. La capacitación debe cubrir la seguridad, las configuraciones, las funciones de seguridad, las acciones de respuesta a incidentes y las operaciones generales de los activos de OT. Si el PWS puede operar manualmente sin el uso de OT, considere agregar capacitación para operaciones manuales. Las operaciones manuales pueden ser una línea de defensa esencial para mantener el PWS operativo en caso de un ciberataque. Hay muchas oportunidades de capacitación en línea disponibles para el personal del PWS, incluidas las de la CISA y la NICCS (consulte los siguientes recursos).

Recursos

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

Norma NIST 800-82. Guía para la seguridad de los sistemas de control industrial: la sección 6.2.2 de la página 6-13 proporciona una guía de capacitación del ICS. *https://csrc.nist.gov/publications/detail/sp/800- 82/rev-2/final*

Capacitación en seguridad cibernética de Federal Virtual Training Environment (FedVTE) de la NICCS: brinda capacitación sobre seguridad cibernética en línea sin costo para empleados gubernamentales estatales, locales, tribales y territoriales. *https://niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte*

Instituto SANS. Capacitación práctica de primer nivel en ICS: esta capacitación de pago ofrece varios cursos diseñados para aumentar las habilidades de seguridad cibernética de quienes usan OT/ICS en su PWS.*https://www.sans.org/cyber-security-courses/?focus-area=industrial-control-systems-security&msc=main-nav*

COSTO: **$**$$$ IMPACTO: **MEDIA** COMPLEJIDAD: **BAJA**

4.5: ¿Acaso el PWS ofrece oportunidades periódicas para fortalecer la comunicación y la coordinación entre el personal de OT y IT, incluidos los proveedores?

Recomendación: organice reuniones entre el personal de OT y IT para que todas las partes comprendan mejor las necesidades de seguridad de la organización y se fortalezcan las relaciones laborales.

¿Por qué es importante este control?

Para garantizar que un PWS satisfaga todas sus necesidades de seguridad cibernética, es fundamental que tanto el personal de OT como el de IT, incluidos los proveedores, comprendan las motivaciones, los desafíos, las necesidades y los objetivos de seguridad cibernética de cada uno. Dado que cada departamento suele usar sistemas de OT y IT y proveedores o personal independiente les dan mantenimiento, los PWS con frecuencia administran la seguridad de estos sistemas por separado. Esta separación puede generar brechas en la seguridad, especialmente con sistemas de OT y IT interconectados. La coordinación y la comunicación periódicas entre el personal de seguridad cibernética de OT y IT pueden ayudar a desarrollar un enfoque más completo de seguridad cibernética de los PWS.

Lineamientos adicionales

- Patrocine al menos una reunión colaborativa por año para el personal de OT y IT. Encontrar una fecha y hora que funcione para todas las partes puede ser difícil, así que programe la reunión con mucha anticipación. Las reuniones presenciales brindan más oportunidades para establecer relaciones.
- Desarrolle una agenda antes de la reunión para que el personal de OT y IT tenga tiempo de preparar sus puntos de discusión. Los temas pueden incluir nuevas actualizaciones de hardware, firmware y software de la OT/IT del PWS; cambios en la arquitectura de la red; informes sobre planes, políticas o procedimientos actualizados; cambios en el personal; funciones y responsabilidades; futuras actividades planificadas de seguridad cibernética; y las amenazas emergentes a la seguridad cibernética.
- Registre los elementos de acción de la reunión, incluido el personal responsable, para que el PWS pueda verificar el estado de los elementos a intervalos regulares.

Consejos de implementación

Los proveedores o contratistas del PWS pueden exigir un pago por su asistencia a la reunión. El PWS debe planificar este costo en su presupuesto. El PWS puede programar la reunión en un día en que los proveedores o contratistas puedan aprovechar para realizar otras actividades en el sitio. Por ejemplo, programe la reunión para el mismo día en que los proveedores planean estar en el PWS a fin de realizar el mantenimiento regular del sistema.

Un simulacro de seguridad cibernética, o un ejercicio de simulación, es una forma impactante de reunir al personal de OT y IT, poner en práctica los planes, políticas y procedimientos existentes y abordar las brechas de seguridad según las lecciones aprendidas del ejercicio. Incluir algunos descansos sociales en el ejercicio puede permitir el desarrollo de relaciones.

Recursos

Herramienta de ejercicios de simulación de la EPA: esta herramienta ayuda a los PWS a diseñar sus propios ejercicios; se proporciona un escenario de seguridad cibernética. *https://ttx.epa.gov/index.html*

Paquetes de ejercicios de simulación de la CISA: estos recursos están diseñados para ayudar a los PWS y otros a realizar sus propios ejercicios. Tenga en cuenta que, en Escenarios de seguridad cibernética, hay uno para los sistemas de agua. *https://www.cisa.gov/cisa-tabletop-exercise-packages*

COSTO: **$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

5.1: ¿Acaso el PWS corrige o mitiga las vulnerabilidades conocidas dentro del plazo recomendado?

Recomendación: identifique y corrija las vulnerabilidades teniendo en cuenta los riesgos (p. ej., los activos fundamentales primero) lo más rápido posible.

¿Por qué es importante este control?

Una vulnerabilidad es una debilidad en una pieza de software o firmware que se ejecuta en un activo de hardware. Las vulnerabilidades pueden provenir de errores en el código o descuidos en el proceso de diseño del software, o los atacantes pueden colocar intencionalmente vulnerabilidades en el software mientras un proveedor escribe el código (es decir, un ataque en la cadena de suministro). Un exploit es un conjunto de acciones o una pieza de código malicioso que los atacantes usan contra la vulnerabilidad, lo que los ayuda a quebrar la seguridad de un sistema informático o dañar un activo.

Cuando un PWS descubre una vulnerabilidad, el creador original del software generalmente trabajará en una nueva versión que no contenga la misma debilidad. La instalación de esta actualización de software se conoce como "parchar" un sistema, y actualizar a la nueva versión evita que un ataque use la vulnerabilidad conocida. Este control es importante porque reduce las posibilidades de que los atacantes aprovechen las vulnerabilidades publicadas para quebrar la seguridad de los sistemas informáticos de un PWS.

Lineamientos adicionales

- En los activos donde no se puedan colocar parches, aplique controles de compensación como la segmentación (es decir, la separación digital de la red en partes más pequeñas, cada una protegida de las demás) y el monitoreo mejorado (p. ej., la instalación de herramientas de monitoreo del tráfico de la red).
- Las medidas aceptables hacen que el activo sea inalcanzable desde la Internet pública o reducen la capacidad de los atacantes para utilizar la vulnerabilidad en un ciberataque.

Consejos de implementación

Para adoptar este control, un PWS puede usar su inventario de activos (consulte la hoja informativa 2.3), la documentación de configuración (consulte la hoja informativa 2.5) y los siguientes recursos para identificar las vulnerabilidades que existen en su sistema. Para los activos de IT, las actualizaciones y parches automatizados a menudo ya están habilitados (p. ej., actualizaciones de Windows). Pero, para los activos de OT, el PWS a menudo desactiva las actualizaciones y parches automáticos. Por lo tanto, es posible que un PWS deba aplicar manualmente actualizaciones y parches para los activos de OT en función de la disponibilidad y la viabilidad operativa. Si un parche no está disponible o interrumpiría de manera inaceptable las operaciones del PWS, un PWS puede usar controles de mitigación como la segmentación de red (consulte la hoja informativa 8.1).

Para ayudar a los PWS a estar al tanto de las vulnerabilidades, el Gobierno federal de EE. UU. mantiene varios recursos de datos de vulnerabilidades de software y puede enviar alertas sobre nuevas entradas a estas bases de datos. La más importante es la base de datos de vulnerabilidades usadas conocidas (KEV)

publicada por la CISA del DHS, que contiene información sobre vulnerabilidades que los atacantes ya están utilizando. Cualquier vulnerabilidad presentada en la KEV debe tratarse con la mayor prioridad. La base de datos nacional de vulnerabilidades (NVD) publicada por el NIST contiene información sobre todas las vulnerabilidades conocidas públicamente. Los PWS también deben registrarse para recibir alertas y avisos del DHS sobre nuevas vulnerabilidades. Si el PWS es miembro de WaterISAC, también recibirá notificaciones de amenazas de seguridad cibernética, incluidas las vulnerabilidades críticas.

Para automatizar el proceso de identificación de vulnerabilidades, la CISA del DHS ofrece servicios gratuitos para sistemas orientados a Internet (consulte la hoja informativa 5.4). Además, muchos proveedores ofrecen herramientas y servicios pagados de identificación de vulnerabilidades para sistemas informáticos internos. Para ayudar en la identificación de vulnerabilidades, un PWS puede usar un identificador de vulnerabilidades en la red de IT y una herramienta de monitoreo pasivo en la red de OT del PWS.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control SI-2 (página 333) y RA-5 (página 242) para obtener más información sobre Corrección de fallas y Monitoreo e identificación de vulnerabilidades.
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Vulnerabilidades usadas conocidas (KEV) de la CISA del DHS: consulte este recurso para ver las vulnerabilidades que los atacantes ya han usado. *https://www.cisa.gov/known-exploited-vulnerabilities- catalog*

Base de datos nacional de vulnerabilidades (NVD) del NIST: consulte este recurso para obtener una lista de vulnerabilidades conocidas públicamente. *https://nvd.nist.gov/vuln/search*

Alertas de la CISA del DHS: consulte este recurso para suscribirse a alertas por correo electrónico del Sistema Nacional de Concientización Cibernética de la CISA del DHS con respecto a nuevas vulnerabilidades.
https://www.cisa.gov/uscert/ncas/alerts

WaterISAC: consulte este recurso para obtener más información sobre el Centro de análisis e intercambio de información (ISAC) sobre el agua. *https://www.waterisac.org/*

COSTO: **$**$$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

5.4: ¿Acaso el PWS garantiza que los activos conectados a la Internet pública no expongan servicios usables innecesarios (p. ej., protocolo de acceso remoto a la computadora)?

Recomendación: elimine los puertos y servicios expuestos innecesarios en los activos de cara al público y revíselos periódicamente.

¿Por qué es importante este control?

Un perímetro de red es el límite seguro entre el lado de la red del PWS (la intranet) y el lado público de la red orientado a Internet. El perímetro contiene los puertos o "entradas" que los atacantes intentan usar para obtener acceso a la intranet de un PWS. Si un PWS conecta un puerto o servicio (es decir, un programa) a Internet, existe una vía para un ataque cibernético y el PWS debe implementar medidas de seguridad para abordarlo.

La violación de las instalaciones de agua de Oldsmar Florida en febrero de 2021 es un ejemplo de un ataque que utiliza software de acceso remoto orientado a Internet (como TeamViewer o Remote Desktop Protocol) para alterar las operaciones del PWS. En el caso de Oldsmar, los atacantes aumentaron la cantidad de hidróxido de sodio en el agua potable a niveles inseguros. Además, los atacantes han utilizado software de acceso remoto expuesto a Internet para introducir ransomware en una computadora de SCADA del PWS. Este control es importante porque cerrar puertos y servicios a la Internet pública ayuda a evitar que los atacantes accedan a la red.

Lineamientos adicionales

- Si un PWS conecta servicios orientados al exterior (p. ej., acceso remoto, alojamiento web) a la Internet pública, el PWS debe implementar controles de compensación apropiados (p. ej., cortafuegos, autenticación de varios factores o registro y monitoreo de actividades) para evitar formas comunes de ataque.

Consejos de implementación

Un PWS puede buscar puertos y servicios expuestos a Internet utilizando Shodan (un motor de búsqueda para activos orientados a Internet) para los activos de su red. Además, la CISA del DHS ofrece servicios gratuitos de exploración de vulnerabilidades que buscan servicios expuestos a Internet y alertan al PWS de los resultados.

A veces, un PWS debe conectarse y, por lo tanto, exponer un servicio o puerto a la Internet pública debido a requisitos operativos. En estos casos, el PWS debe usar un servicio de MFA (por ejemplo, Duo, Okta, RSA) para restringir el acceso a los usuarios autorizados y un cortafuegos para filtrar el tráfico inusual; además, el PWS debe monitorear el acceso a la red y los registros de actividad para detectar acciones inusuales que puedan indicar un ciberataque.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control AC-17 (página 48) y SC-7 (página 297) para obtener más información sobre

Acceso remoto y Protección de límites. *https://csrc.nist.gov/publications/detail/sp/800- 53/rev-5/final*

Alerta AA21-042A y AA21-287A de la CISA del DHS: consulte estos recursos para obtener información sobre varias infracciones del sistema de agua de 2019 a 2021, incluida la de la planta de agua de Oldsmar en Florida. *https://www.cisa.gov/uscert/ncas/alerts/aa21-042a*; *https://www.cisa.gov/uscert/ncas/alerts/aa21-287a*

Servicios de higiene cibernética de la CISA del DHS: consulte este recurso para obtener más información sobre el servicio gratuito de análisis de vulnerabilidades del DHS. *https://www.cisa.gov/cyber-hygiene-services*

Shodan: consulte este recurso para buscar activos conectados a Internet en la red del PWS. *https://www.shodan.io/*

Gestión de vulnerabilidades: restricción de las conexiones de OT a la Internet pública

COSTO: **$$$** $ IMPACTO: **MEDIA** COMPLEJIDAD: **MEDIA**

5.5: ¿Acaso el PWS elimina las conexiones entre sus activos de OT e Internet?

Recomendación: elimine las conexiones de activos de OT a la Internet pública, a menos que se requieran explícitamente para las operaciones.

¿Por qué es importante este control?

Los desarrolladores no diseñaron los sistemas de SCADA y OT teniendo en cuenta la seguridad, los PWS no los parchan ni los actualizan regularmente, y conectarlos directamente a Internet puede representar un riesgo de seguridad cibernética importante para las operaciones del PWS. Por lo tanto, un aspecto crucial de la seguridad cibernética del PWS es saber qué activos de SCADA u OT ha conectado el PWS a Internet y eliminar dicha conexión a Internet si es posible.

Si bien un PWS siempre debe evitar conectar los activos de OT a Internet, las necesidades operativas (p. ej., la administración de sitios remotos) a veces pueden requerir estas conexiones. El PWS puede reducir el riesgo cibernético que estas conexiones representan a través de controles de compensación como MFA, cortafuegos y registro centralizado.

Lineamientos adicionales

- Para identificar si un PWS ha conectado activos de OT a Internet, evalúe tanto la conectividad estándar (p. ej., la red de SCADA conectada a la red de IT o el módem de Internet) como otros métodos (p. ej., inalámbrico o celular) para conectar los activos de OT a Internet.
- Un PWS debe justificar formalmente las conexiones de Internet a cualquier activo de OT e incluir controles de compensación.

Consejos de implementación

Como se menciona en la hoja informativa 5.4, un PWS puede buscar activos de OT expuestos a Internet mediante el uso de los servicios gratuitos de identificación de vulnerabilidades de Shodan o la CISA del DHS. Un ejemplo de una conexión que se pasa por alto fácilmente entre los sistemas de OT e Internet es el uso de módems celulares para conectar activos remotos (p. ej., tanques, estaciones de bombeo, pozos) al sistema de SCADA principal. Cuando se usan, los módems celulares deben estar en las redes privadas del proveedor de telecomunicaciones siempre que sea posible.

El PWS debe crear un proceso para justificar y documentar la necesidad operativa de una conexión de OT a Internet con el líder de seguridad cibernética de la OT. Cuando las necesidades operativas requieran una conexión de OT a Internet aprobada, el PWS debe usar los controles de compensación detallados en la hoja informativa 5.4 para mitigar el riesgo cibernético que crea esta conexión.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control AC-17 (página 48) y SC-7 (página 297) para obtener más información sobre Acceso remoto y Protección de límites.
https://csrc.nist.gov/publications/detail/sp/800- 53/rev-5/final

Servicios de higiene cibernética de la CISA del DHS: consulte este recurso para obtener más información sobre el servicio gratuito de análisis de vulnerabilidades del DHS.
https://www.cisa.gov/cyber-hygiene-services

Shodan: consulte este recurso para buscar activos conectados a Internet en la red del PWS.
https://www.shodan.io/

COSTO: **$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

6.1: ¿Acaso el PWS incluye la seguridad cibernética como criterio de evaluación para contratar bienes y servicios de OT y IT?

Recomendación: incluya la seguridad cibernética como criterio de evaluación en la adquisición de bienes y servicios.

¿Por qué es importante este control?

Otorgar acceso a un proveedor a una red del PWS para realizar un servicio (p. ej., mantenimiento, cambios de configuración) o instalar nuevo hardware o software puede crear una nueva manera para que los atacantes vulneren la red. En muchas circunstancias, es más conveniente y rentable para un proveedor acceder de forma remota a una red sin estar físicamente presente en el PWS. Sin embargo, si el proveedor no protege de manera eficaz sus propios sistemas informáticos, cualquier malware o infección en los sistemas del proveedor puede migrar a los del PWS.

El hardware o software instalado puede tener debilidades no intencionales (es decir, vulnerabilidades) que un atacante puede usar para ingresar a un sistema. Además, un atacante (con el conocimiento del proveedor o sin este) puede insertar intencionalmente vulnerabilidades en el hardware o software para introducir una debilidad en la red del PWS. El ataque SolarWinds de 2020 es un ejemplo de un ataque de este tipo que afectó a varias agencias del Gobierno federal.

Las preocupaciones de que los gobiernos extranjeros puedan colocar intencionalmente debilidades en los productos de hardware exportados desde su país han llevado a la Comisión Federal de Comunicaciones (FCC) a prohibir a ciertos proveedores trabajar en las redes del Gobierno federal de EE. UU., así como en la importación y la venta en EE. UU. La implementación de este control ayudará al PWS a comprar más productos y servicios seguros, y reducir así el riesgo cibernético.

Lineamientos adicionales

- Dadas dos ofertas de costo y función más o menos similares, el PWS debe dar preferencia a la oferta o al proveedor más seguro.
- Si un PWS busca adquirir nuevos activos de IT u OT, incluya los requisitos de seguridad cibernética en el proceso de adquisición en la etapa más temprana para que los proveedores que respondan a la solicitud de oferta sepan que deben cumplir con estos requisitos por anticipado.

Consejos de implementación

Si un PWS otorga a un proveedor acceso remoto a una red, el PWS debe exigir al proveedor que utilice técnicas seguras, como una red privada virtual (VPN) y MFA. El PWS también puede implementar cortafuegos para filtrar el tráfico inusual, así como monitorear y registrar la actividad de la red. El siguiente recurso del Departamento de Energía presenta ejemplos de frases de contratación para los requisitos de seguridad cibernética de los proveedores que los PWS pueden insertar en los contratos de los proveedores.

Para evaluar a los proveedores de hardware y software y reducir el riesgo cibernético que representan para los activos del PWS, los empleados del PWS pueden preguntar a los proveedores sobre sus prácticas e investigaciones de seguridad cibernética en línea con el fin de hacerse una idea de su seguridad cibernética general.

Un PWS puede usar avisos gubernamentales para investigar proveedores potenciales, así como buscar bases de datos de vulnerabilidades (es decir, vulnerabilidades usadas conocidas [KEV] y base de datos nacional de vulnerabilidades [NVD]) (consulte la hoja informativa 5.1).

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control SR-6 (página 369) y SR-5 (página 368) para obtener más información sobre Evaluaciones y revisiones de proveedores y Estrategias, herramientas y métodos de adquisición. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

GAO-22-104746. Respuesta federal a los incidentes de SolarWinds y Microsoft Exchange: consulte la sección Qué encontró la GAO para obtener más información sobre el ataque a la cadena de suministro de SolarWinds de 2020. *https://www.gao.gov/products/gao-22-104746*

Vulnerabilidades usadas conocidas (KEV) de la CISA del DHS: consulte este recurso para ver las vulnerabilidades que los atacantes ya han usado. *https://www.cisa.gov/known-exploited-vulnerabilities-catalog*

Base de datos nacional de vulnerabilidades (NVD) del NIST: consulte este recurso para obtener una lista de vulnerabilidades conocidas públicamente. *https://nvd.nist.gov/vuln/search*

FCC. Prohibiciones de hardware de proveedores promulgadas: Consulte estos recursos para obtener detalles sobre las prohibiciones actuales de hardware de proveedores.

https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats

https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat

Frases para la contratación de seguridad cibernética del Departamento de Energía (DOE): consulte este recurso para ver ejemplos de frases para la contratación de seguridad cibernética que incluir en los contratos de proveedores. *https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april- 2014*

Alertas de la CISA del DHS: consulte este recurso para suscribirse a alertas por correo electrónico del Sistema Nacional de Concientización Cibernética de la CISA del DHS con respecto a nuevas vulnerabilidades.
https://www.cisa.gov/uscert/ncas/alerts

Cadena de suministro/terceros: informe de incidentes de la cadena de suministro y divulgación de vulnerabilidades

COSTO: **$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

6.2/6.3: ¿Acaso el PWS requiere que todos los vendedores y proveedores de servicios de OT y IT notifiquen al PWS sobre cualquier incidente de seguridad o vulnerabilidad en un período que considere el riesgo?

Recomendación: exija a los vendedores y los proveedores de servicios que notifiquen al PWS sobre posibles incidentes de seguridad y vulnerabilidades dentro de un plazo estipulado indicado en los documentos y contratos de adquisición.

¿Por qué es importante este control?

La hoja informativa 6.1 analiza el riesgo cibernético que los proveedores pueden representar para una red de PWS. Si un proveedor de software o hardware no integra la seguridad en el diseño del producto o es víctima de un ciberataque (p. ej., el ataque de SolarWinds de 2020), el proveedor puede introducir debilidades (es decir, vulnerabilidades) en los sistemas informáticos del PWS. En ese caso, un atacante puede usar esas vulnerabilidades en el PWS.

Si bien muchos proveedores comparten la información de manera proactiva a los clientes, algunos proveedores pueden dudar u ocultar el descubrimiento de incidentes de seguridad o vulnerabilidades en sus productos debido a la incertidumbre o preocupaciones de responsabilidad. Recibir notificaciones oportunas sobre los incidentes y vulnerabilidades de seguridad del proveedor brinda al PWS la oportunidad de prevenir o responder a posibles ataques; por lo tanto, los PWS deben incluir un requisito de notificación contractual en los documentos de adquisición.

Lineamientos adicionales

- Al comprobar los requisitos de seguridad cibernética dentro de los contratos, revise tanto los contratos de proveedores de servicios como los acuerdos de proveedores de hardware/software (p. ej., integrador de OT, proveedor de IT).

Consejos de implementación

Para garantizar que otras organizaciones cumplan con sus responsabilidades de notificación, los PWS pueden incluirlas en los contratos de adquisición de productos de hardware y software y en los acuerdos de nivel de servicio (SLA) para los servicios. El PWS puede elegir un período razonable y basado en el riesgo en el que espera que el proveedor notifique al PWS sobre vulnerabilidades recién descubiertas en los productos que el proveedor ofrece y ataques cibernéticos en los sistemas informáticos del proveedor. Luego, el PWS puede incluir cláusulas que requieran estos plazos de notificación en sus futuros contratos de adquisición y SLA con los proveedores, así como las sanciones si el proveedor no cumple con estos requisitos.

El siguiente recurso del Departamento de Energía presenta ejemplos de frases de contratación para los requisitos de seguridad cibernética de los proveedores que los PWS pueden insertar en los contratos de los proveedores.

Recursos

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control SR-8 (página 371) para obtener más información sobre Acuerdos de notificación. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

GAO-22-104746. Respuesta federal a los incidentes de SolarWinds y Microsoft Exchange: consulte la sección Qué encontró la GAO para obtener más información sobre el ataque a la cadena de suministro de SolarWinds de 2020. *https://www.gao.gov/products/gao-22-104746*

Frases para la contratación de seguridad cibernética del Departamento de Energía (DOE): consulte la sección 3.3 del Informe de problemas dentro de este recurso para ver un ejemplo de frases sobre seguridad cibernética que incluir en los contratos de los proveedores. *https://www.energy.gov/ceser/articles/cybersecurity-procurement-language- energy-delivery-april-2014*

COSTO: **$**$$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

7.1: ¿Acaso el PWS tiene un procedimiento escrito para reportar incidentes de seguridad cibernética que indique el medio (p. ej., llamada telefónica, envío por Internet) y el destinatario (p. ej., FBI u otras fuerzas del orden público, la CISA, reguladores estatales, WaterISAC, un proveedor de seguros cibernéticos)?

Recomendación: documente el procedimiento a fin de informar incidentes de seguridad cibernética con prontitud para contribuir con la aplicación de la ley, recibir asistencia con la respuesta y la recuperación, y promover la conciencia del sector del agua sobre las amenazas de seguridad cibernética.

¿Por qué es importante este control?

Informar incidentes a agencias externas puede ayudar a los PWS a responder mejor y recuperarse de un incidente de seguridad cibernética. La información reportada también puede ayudar a evitar que el ciberdelito ocurra en otros PWS y organizaciones. WaterISAC y los centros de fusión locales o estatales también fomentan la denuncia de incidentes cibernéticos y actividades sospechosas, ya que las autoridades pueden analizar la información para ayudar a compartir información sobre tendencias y conciencia al sector del agua.

Lineamientos adicionales

- Desarrolle un procedimiento y una plantilla de informe para reportar los incidentes de seguridad cibernética con prontitud.
- Identifique al personal del PWS que envía informes a organizaciones externas.
- Especifique los procedimientos de escalamiento (p. ej., a quién notifica el PWS, cuándo y por qué) para enviar informes a las organizaciones externas identificadas y los plazos para compartir la información. Los diagramas de flujo u otras imágenes pueden ayudar al personal del PWS a comprender en qué orden deben notificar a los demás y qué información deben reportar.
- Distribuya el procedimiento de informes y la plantilla al personal del PWS. Incluya esta información en otros documentos de respuesta a emergencias, como el plan de respuesta a emergencias del PWS o el plan de respuesta a incidentes de seguridad cibernética.
- Según la Ley de Informes de Incidentes Cibernéticos para Infraestructura Crítica de 2022, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) del Departamento de Seguridad Nacional (DHS) de EE. UU. establecerá procedimientos que pueden aplicarse a los PWS. La EPA revisará esta guía según sea necesario cuando la CISA publique esos procedimientos.
- Si el PWS se suscribe a un seguro cibernético o tiene un anticipo de respuesta a incidentes cibernéticos, incluya a estos proveedores como contactos dentro del procedimiento escrito. A menudo, se requieren plazos de presentación de informes asociados con la presentación de reclamos contra seguros cibernéticos o anticipos de respuesta a incidentes.

Consejos de implementación

El procedimiento escrito debe incluir lo siguiente:

- Información de contacto para enviar los informes a las siguientes entidades: o La agencia local de aplicación de la ley del PWS.

- CISA del DHS: las organizaciones afectadas deben enviar un informe de incidente de la CISA en línea, enviar un correo electrónico a report@cisa.gov o llamar al 888-282-0870.
- El Buró Federal de Investigaciones (FBI): las organizaciones afectadas deben comunicarse con la oficina local del FBI más cercana o enviar un informe a través del Centro de Denuncias de Delitos en Internet (IC3) de la Oficina.
- El WaterISAC y los centros de fusión locales/estatales: para informar a WaterISAC, el PWS puede enviar un informe de WaterISAC en línea, enviar un correo electrónico a analista@waterisac.org, o llamar al 866426-4722.
- El proveedor de seguros cibernéticos del PWS o el titular del anticipo de respuesta a incidentes cibernéticos (si corresponde).

La plantilla del informe debe incluir lo siguiente:

- fecha y hora en que el PWS detectó el incidente;
- fecha y hora en que ocurrió el incidente;
- breve descripción del incidente, incluida la identificación del posible método de ataque;
- lista de activos afectados;
- identificación de cualquier información de identificación personal (PII) que el incidente pueda haber comprometido;
- fecha, hora y descripción de la respuesta o acciones correctivas que el PWS realizó;
- personal o proveedores del PWS involucrados en la detección y respuesta de incidentes.

Cualquier información que el PWS comparta con el DHS o el FBI, o cualquier otra agencia del Gobierno federal, es información de infraestructura crítica protegida (PCII) y esas agencias no la compartirán con el público. Para obtener más información, consulte la hoja informativa de PCII de la CISA.

Recursos

Envío de informes a la CISA: proporciona información sobre cómo informar incidentes y actividades sospechosas.

https://www. cisa.gov/report

Envío de informes al FBI: proporciona información sobre cómo enviar informes de delitos cibernéticos. *https://www.fbi.gov/investigate/cyber*

Envío de informes a WaterISAC: proporciona información sobre cómo informar incidentes y actividades sospechosas. *https://www.waterisac.org/report-incident*

Hoja informativa de PCII de la CISA: explica las protecciones que ofrece el programa de PCII. *https://www.cisa.gov/publication/pcii-fact-sheet*

COSTO: **$**$$$ IMPACTO: **ALTO** COMPLEJIDAD: **BAJA**

7.2: ¿Acaso el PWS tiene un plan escrito de respuesta a incidentes de seguridad cibernética (IR) para escenarios de amenazas críticas (p. ej., desactivación o manipulación de sistemas de control de procesos, pérdida o robo de datos operativos o financieros, exposición de información confidencial), que se ponga en práctica y se actualice con regularidad?

Recomendación: desarrolle, ponga en práctica y actualice un plan de IR para los incidentes de seguridad cibernética que podrían afectar las operaciones de PWS. Realice simulacros para mejorar las respuestas a posibles incidentes cibernéticos.

¿Por qué es importante este control?

El plan de IR de un PWS presenta las estrategias, los recursos y los procedimientos de este para prepararse y responder ante un incidente cibernético. El plan de IR de seguridad cibernética es esencial para ayudar a un PWS a recuperarse rápidamente de los incidentes de seguridad cibernética. El PWS puede incluir el plan de IR en su Plan de Respuesta a Emergencias (ERP).

Lineamientos adicionales

- Identifique el personal, el personal de apoyo de OT y IT y los proveedores que el PWS debe incluir en el desarrollo o actualización del plan de IR.
- Desarrolle el plan de IR de seguridad cibernética para que incluya lo siguiente:
  - Funciones y responsabilidades definidas y acciones que todo el personal de PWS realizará durante un incidente y después de este.
  - Procedimientos para operar el PWS en modo manual, o procedimientos alternativos para mantener el servicio de agua si un ataque afecta el sistema de OT.
  - Referencias a otros planes y procedimientos de respuesta relevantes según sea necesario.
  - Diagramas y otros elementos visuales para ayudar a todo el personal del PWS a comprender sus funciones, responsabilidades y acciones.
  - Plantillas de formularios que el personal del PWS puede usar para registrar decisiones, acciones y gastos.
  - Procedimientos e información de contacto sobre dónde reportar el incidente (consulte la hoja informativa 7.1)
- Distribuya el plan de IR y capacite a todo el personal del PWS sobre los nuevos procedimientos o pasos de seguridad cibernética en el plan de IR. Un método para capacitar al personal del PWS es realizar simulacros y ejercicios.
- Revise el plan de IR anualmente, como mínimo, y realice los cambios necesarios, como modificaciones en el personal, los proveedores y la información de contacto.
- Actualice el plan de IR después de que ocurra cualquier cambio significativo en los sistemas de OT y IT del PWS y en base a las lecciones aprendidas en una simulación o incidente real.

Consejos de implementación

Un buen punto de partida para desarrollar un plan de IR es la Lista de verificación de acciones en caso de incidentes de seguridad cibernética de la EPA. Realizar simulacros y ejercicios regulares, como ejercicios de simulación, es esencial para tener una respuesta de emergencia efectiva y minimizar los impactos adversos de un incidente cibernético. El PWS debe planificar y realizar ejercicios con la participación del personal del PWS, personal de apoyo de OT y IT, proveedores y socios de respuesta ante emergencias. Si los simulacros y ejercicios son nuevos para el PWS, use un escenario que sea simple y realista. Por ejemplo, desarrolle un escenario que se base en un ataque de ransomware, ya que es un método de ataque común. El objetivo es ejercitar y evaluar los planes, políticas y procedimientos existentes y actualizarlos con las lecciones aprendidas. La realización de ejercicios también ayudará a desarrollar las capacidades de respuesta ante ciberataques del PWS. Después de realizar los ejercicios, el PWS debe realizar un informe sobre el ejercicio. El informe brinda una oportunidad para que los participantes del ejercicio comenten sobre lo que sucedió durante el ejercicio y los obstáculos o desafíos encontrados, y para identificar las brechas en los planes, las políticas y los procedimientos del PWS que se deben abordar.

Recursos

Plantilla e instrucciones del Plan de Respuesta a Emergencias de la EPA: proporciona una plantilla y un documento de instrucciones para los PWS.
https://www.epa.gov/waterutilityresponse/develop-or-update- emergency-response-plan

Lista de verificación de acciones en caso de incidentes para la seguridad cibernética de la EPA: proporciona una lista de verificación práctica para ayudar a los PWS a prepararse, responder y recuperarse ante incidentes cibernéticos. *https://www.epa.gov/sites/default/files/2017-11/documents/171013- incidentactionchecklist-cybersecurity_form_508c.pdf*

15 aspectos fundamentales de la seguridad cibernética de WaterISAC: la página 35 proporciona información y recursos para desarrollar un plan de IR.
https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf

Herramientas de respuesta ante incidentes cibernéticos de la CISA: proporciona capacitación y manuales de respuesta ante incidentes.

https://www. cisa. gov/cyber-incident-response

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

COSTO: **$$**$$ IMPACTO: **ALTO** COMPLEJIDAD: **MEDIA**

7.3: ¿Acaso el PWS hace copias de seguridad de los sistemas necesarios para las operaciones (p. ej., configuraciones de red, lógica de PLC, planos de ingeniería, registros de personal) de manera regular, guarda las copias de seguridad por separado de los sistemas originales y los prueba periódicamente?

Recomendación: realice copias de seguridad de los sistemas de OT y IT fundamentales de PWS, guárdelas de manera segura y por separado, y pruébelas.

¿Por qué es importante este control?

Las copias de seguridad son un elemento crucial de las actividades de restauración y recuperación de un PWS en caso de un incidente cibernético, mal funcionamiento del hardware (p. ej., falla del disco duro) o destrucción física del equipo (p. ej., incendio o inundación). Dado que el ransomware es una amenaza cibernética clave para los PWS, en la que los atacantes buscan cifrar archivos y dejarlos inutilizables, 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.

Lineamientos adicionales

- Identifique todos los datos operativos, de clientes, de empleados, financieros y de otro tipo que un PWS pueda perder o que un atacante pueda corromper durante un incidente, y que el PWS necesitaría restaurar después del incidente para reanudar las operaciones normales.
- El PWS debe almacenar las copias de seguridad por separado de los sistemas que se respaldan siempre que sea posible. Este método no solo protegerá los datos en caso de un incidente cibernético, sino también en caso de incidentes como un incendio o una inundación. Este método se puede realizar utilizando copias de seguridad fuera del sitio, basadas en la nube o rotaciones de copias de seguridad manuales (p. ej., tener varias unidades de copia de seguridad e intercambiarlas periódicamente a la vez que el PWS guarda una de manera externa).
- Establezca un procedimiento para asegurarse de que el PWS siga el proceso de copia de seguridad según el cronograma especificado y que las copias de seguridad de archivos sean utilizables. Como mínimo, estas acciones deben incluir verificar de manera puntual el tamaño del archivo y la fecha de modificación de los archivos de la copia de seguridad en los medios de recuperación o validar que el PWS puede recuperar los archivos individualmente.
- Para los activos de OT, asegúrese de que las copias de seguridad incluyan elementos como lógica de PLC y gráficos HMI para que el PWS también pueda restaurarlos rápidamente.
- Como mínimo, el PWS debe hacer copias de seguridad de los sistemas y probar dichas copias anualmente.

Consejos de implementación

El PWS debe realizar copias de seguridad mediante el enfoque de copia de seguridad en profundidad, con capas de copias de seguridad (p. ej., local, instalación, desastre) secuenciadas en el tiempo, de modo que las copias de seguridad locales recientes estén disponibles para uso inmediato y las copias de seguridad protegidas estén disponibles para la recuperación ante un gran incidente de seguridad cibernética. El enfoque de copia 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 distintos y guarde como mínimo una copia de forma remota externamente o en la nube.

El PWS debe usar varios métodos de almacenamiento y enfoques de copias de seguridad o recuperación para asegurar la producción rigurosa, el almacenamiento seguro y el acceso adecuado a las copias de seguridad para su recuperación.

Recursos

Norma 800-82 del NIST. Guía para la seguridad del sistema de control industrial (ICS): puede encontrar información adicional sobre la redundancia y la tolerancia a fallas en la sección 5.13 (página 5-21). *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*

Norma NIST 800-34. Guía de planificación de contingencia para sistemas de información federales:
puede encontrar información adicional sobre los procedimientos generales de copia de seguridad y las prácticas recomendadas en la sección 3.4.2 (página 21).
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800- 34r1.pdf

Respuesta y recuperación: topología de la red de documentos

COSTO: **$$**$$ IMPACTO: **MEDIA** COMPLEJIDAD: **MEDIA**

7.4: ¿Acaso el PWS mantiene documentación actualizada que describe la topología de la red (es decir, las conexiones entre todos los componentes de la red) a través de las redes de OT y IT del PWS?
Recomendación: conserve una documentación completa y precisa de todas las topologías de redes de IT y OT del PWS para facilitar la respuesta y la recuperación ante incidentes.

¿Por qué es importante este control?

Una topología de red bien definida ayuda a los administradores de sistemas a localizar fallas, solucionar problemas y asignar recursos de red. Los diagramas o topologías de red son un punto de referencia importante para diagnosticar problemas de red e identificar posibles vulnerabilidades de seguridad, ya que representan los diseños físicos y lógicos. Un diagrama de red lógico completo y actualizado es esencial para la recuperación ante desastres cibernéticos.

Lineamientos adicionales

- Para crear una topología de red precisa, el PWS debe realizar una encuesta de red a fin de validar cualquier vía de conexión conocida y desconocida anteriormente. Al realizar este estudio, incluya no solo las conexiones de red tradicionales basadas en Ethernet; busque también rutas menos tradicionales, como comunicaciones en serie, inalámbricas, de acceso telefónico y de trayectoria óptica. Cuando haya activos remotos (p. ej., tanques, estaciones de bombeo), evalúe cómo estos se comunican con la red del PWS.
- Después de que el PWS complete la encuesta de la red, registre los resultados y manténgalos actualizados. Las redes del PWS pueden ser bastante complejas y los resultados de los estudios documentados ayudarán a garantizar que el PWS no pase por alto ni olvide los canales de comunicación con el tiempo. La documentación de los estudios debe incluir detalles sobre los activos específicos de la red, las conexiones y el método utilizado para la conexión (p. ej., cableado, inalámbrico). El PWS debe centrarse especialmente en los sistemas que se conectan directamente a la Internet pública y cualquier vía de comunicación entre los sistemas de OT (p. ej., SCADA) y IT (es decir, la empresa comercial).

Consejos de implementación

Para ser eficiente, un PWS puede realizar un estudio de la red al mismo tiempo que revisa la configuración de activos detallada en la hoja informativa 2.5 y el proceso de inventario de activos detallado en la hoja informativa 2.3. Lucidchart es un sitio web gratuito y fácil de usar que puede ayudar a crear diagramas de red. Microsoft proporciona un breve desglose de lo que se debe incluir en un diagrama de red. La herramienta de evaluación de ciberseguridad (CSET) de la CISA es una versión gratuita de gráficos básicos relacionados con Visio y OT para crear topologías de red.

Considere incluir el diagrama de red en el Plan de Respuesta a Incidentes (IR) de Seguridad Cibernética del PWS, o Plan de Respuesta a Emergencias, ya que esta información puede ser valiosa para la respuesta a incidentes.

Recursos

Lucidchart: es una aplicación de creación de diagramas de la web que permite a los usuarios colaborar visualmente para dibujar, revisar y compartir gráficos y diagramas, y mejorar procesos, sistemas y estructuras organizacionales.

https://www.lucidchart.com/pages/examples/diagram-maker

Microsoft. Creación de un diagrama de red básico: si el PWS usa el software Microsoft Visio, esta página describe cómo la plantilla de diagrama de red básica incluye formas estándar para servidores, computadoras y otras partes de una red de un PWS.

https://support.microsoft.com/en-us/office/create-a-basic-network-diagram-f2020ce6-c20f-4342-84f7-bf4e7488843a

Herramienta CSET de la CISA: esta aplicación de escritorio independiente guía a un PWS a través de un proceso sistemático de evaluación de sus activos de OT y IT, incluida la creación de diagramas de red.

https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

Otras medidas de seguridad: segmentación de la red

COSTO: **$$$**$ IMPACTO: **ALTO** COMPLEJIDAD: **ALTO**

8.1: ¿Acaso el PWS segmenta las redes de OT y IT y rechaza las conexiones a la red de OT de forma predeterminada, a menos que se autoricen explícitamente (p. ej., por dirección IP y puerto)?

Recomendación: requiera que las conexiones entre las redes de OT y IT pasen a través de un intermediario, como un cortafuegos, un servidor bastión, una caja de salto o una zona desmilitarizada, que se monitorea y registra.

¿Por qué es importante este control?

Dado que las organizaciones usaban redes de OT mucho antes de la invención de Internet, sus fabricantes no los diseñaron con el mismo nivel de seguridad que las redes de IT. A medida que Internet se hizo popular, las organizaciones normalmente mantuvieron las redes de OT separadas de los sistemas de IT y dejaron así lo que se denomina un "espacio libre" entre las redes de OT y IT. Sin embargo, con el tiempo, las organizaciones se dieron cuenta de que podían hacer sus operaciones más eficientes y ahorrar costos al conectar los sistemas de OT y IT y compartiendo datos entre ellos.

Si bien el concepto de un espacio libre sigue siendo una respuesta popular a las preocupaciones de seguridad de la conectividad de OT/IT, es prácticamente imposible mantener uno incluso en las instalaciones más seguras (p. ej., Stuxnet, 2010). Por lo tanto, la mayoría de los ataques cibernéticos que tienen como objetivo las redes de OT comienzan como ataques a la red de IT de un PWS.

La segmentación es una práctica de seguridad que divide digitalmente las redes informáticas de OT y IT de un PWS con el objetivo de mejorar el rendimiento de la red y la seguridad cibernética. Este control es importante porque un PWS puede limitar la capacidad de un atacante para acceder a los sistemas de control de la OT después de afectar la red de IT.

Lineamientos adicionales

- Solo permita conexiones a la red de OT desde la red de IT a través de activos aprobados y otros medios autorizados.
- De manera predeterminada, rechace todas las conexiones a la red de OT desde la red de IT, a menos que se autoricen explícitamente (por dirección IP y puerto) para una función específica del sistema.

Consejos de implementación

Un marco útil para comprender dónde segmentar la red es la arquitectura de referencia empresarial de Purdue (PERA), o el modelo de Purdue para abreviar. Este modelo separa las redes de OT y IT en capas, lo que ayuda a diferenciar los tipos de activos en cada nivel de una red de sistema de control. Los niveles 0 a 3 consisten en activos de OT, y los niveles 4 y 5 se refieren a la red empresarial de IT.

La segmentación de la red ocurre principalmente entre las redes de OT y IT de los niveles 3 y 4, donde un PWS puede establecer una "zona desmilitarizada" como un búfer entre las redes de OT y IT mediante el uso de herramientas de hardware y software para monitorear, registrar y filtrar el tráfico. La herramienta más común que un PWS puede usar para la segmentación de la red es instalar un cortafuegos en el límite de las redes de OT y IT, que puede rechazar todas las conexiones entre los sistemas de OT y IT de forma predeterminada.

Con un cortafuegos, un PWS puede controlar el flujo de información entre subredes o sistemas por tipo de tráfico, origen, destino y otras opciones.

Recursos

Norma 800-82 del NIST (revisión 2). Guía para la seguridad del sistema de control industrial (ICS): consulte la sección 5.1 (página 5-1) para obtener más información sobre Segmentación y segregación de la red. *https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final*

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control AC-4 (página 28) y SC-7 (página 297) para obtener más información sobre Cumplimiento del flujo de información y Protección de límites.

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Recomendación de la Agencia de Seguridad Nacional (NSA) para detener la actividad cibernética maliciosa contra la OT conectada: esta recomendación presenta las medidas que un PWS puede tomar para evaluar los riesgos contra su sistema de OT que pueden darse mediante la conexión del sistema de IT e implementar cambios con los recursos actuales para monitorear y detectar de manera realista la actividad maliciosa. *https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA- AGAINST-OT UOO13672321.PDF*

MITRE ATT&CK. Stuxnet: consulte Replicación a través de medios extraíbles para obtener más información sobre la propagación de Stuxnet. *https://attack.mitre.org/software/S0603/*

Instituto SANS. El modelo de Purdue y las prácticas recomendadas para proteger arquitecturas de ICS:
consulte este recurso para obtener más información sobre el modelo de Purdue y dónde se produce la segmentación de red en una red de OT. *https://www.sans.org/blog/introduction-to-ics- security-part-2/*

CISA del DHS. Comprensión de los cortafuegos para uso doméstico y de oficina pequeña: consulte este recurso para obtener más información sobre cómo seleccionar y configurar un cortafuegos. *https://www.cisa.gov/tips/st04- 004*

COSTO: **$$$**$ IMPACTO: **MEDIA** COMPLEJIDAD: **ALTO**

8.2: ¿Acaso el PWS mantiene una lista de amenazas y tácticas, técnicas y procedimientos (TTP) usados por los delincuentes a fin de realizar ataques cibernéticos relevantes para el PWS y tiene la capacidad de detectar eventos de amenazas clave?

Recomendación: reciba alertas de la CISA y mantenga la documentación de los TTP relevantes para el PWS.

¿Por qué es importante este control?

Los ataques cibernéticos necesitan varios pasos para ingresar y moverse dentro de un sistema informático del PWS. Los atacantes suelen emplear pasos o métodos comunes durante un ciberataque, conocidos como TTP. Si un PWS conoce los TTP comunes, puede monitorearlos en la red del PWS y detectar un ataque antes de que interrumpa o dañe las operaciones.

El PWS debe monitorear los componentes externos e internos como parte de su programa de seguridad cibernética de OT y IT. El monitoreo externo observa eventos en el límite de la red, y el monitoreo interno captura eventos dentro de los sistemas del PWS. Este control es importante porque ayuda a un PWS a conocer y detectar amenazas a sus redes de OT y IT.

Lineamientos adicionales

- Adopte las medidas y mitigaciones recomendadas en las alertas de la CISA, como reglas de filtrado de tráfico de cortafuegos, alertas de tráfico de red sospechoso o sistemas comerciales de prevención y detección para detectar amenazas clave cuando sea posible.
- Si un PWS identifica una amenaza validada dentro de la red de IT u OT, el PWS debe seguir su plan de respuesta ante incidentes (consulte la hoja informativa 7.2) para contener, eliminar y recuperarse de la amenaza.

Consejos de implementación

Las alertas y los avisos brindan información oportuna sobre problemas de seguridad cibernética actuales y TTP, vulnerabilidades y exploits. Regístrese para recibir alertas y avisos por correo electrónico de la CISA del DHS. Otras fuentes útiles para comprender los TTP y las acciones que un atacante puede realizar para moverse a través de una red de OT o IT son MITRE ATT&CK y MITRE ATT&CK para marcos de ICS, respectivamente.

Existen muchas herramientas disponibles comercialmente que un PWS puede usar para monitorear ciertos tipos de ataques cibernéticos o intrusiones en la red del PWS. Estas herramientas incluyen sistemas de detección de intrusiones/sistemas de prevención de intrusiones (IDS/IPS), reglas de cortafuegos que filtran y alertan sobre cierto tráfico y herramientas de monitoreo de la red de ICS.

Estas herramientas pueden enviar alertas a un sistema de monitoreo central, a menudo llamado herramienta de control de eventos e información del sistema (SIEM).

Una herramienta de SIEM extrae datos de muchas fuentes (p. ej., IDS/IPS, cortafuegos, herramientas de monitoreo de red, eventos de Windows) en un panel y puede alertar al PWS sobre actividad de red inusual o maliciosa.

Recursos

Norma 800-82 del NIST (revisión 2). Guía para la seguridad del sistema de control industrial (ICS): consulte la sección 6.2.17 (página 6-38) para obtener más información sobre Integridad del sistema y de la información.

https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control SI-4 (página 336) para obtener más información sobre Monitoreo del sistema. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Alertas de la CISA del DHS: consulte este recurso para suscribirse a alertas por correo electrónico del Sistema Nacional de Concientización Cibernética de la CISA del DHS con respecto a nuevas vulnerabilidades.

https://www.cisa.gov/uscert/ncas/alerts

MITRE ATT&CK y MITRE ATT&CK para ICS: consulte estos recursos para obtener más información sobre los TTP comunes en sistemas de OT y IT, respectivamente.
https://attack.mitre.org/matrices/ics/; https://attack.mitre.org/matrices/enterprise/

COSTO: **$** $$$ IMPACTO: **MEDIA** COMPLEJIDAD: **BAJA**

8.3: ¿Acaso el PWS utiliza controles de seguridad de correo electrónico para reducir las amenazas comunes presentadas por los correos electrónicos, como la suplantación de identidad, el phishing y la interceptación?

Recomendación: asegúrese de que los controles de seguridad del correo electrónico estén habilitados en toda la infraestructura de correo electrónico corporativa.

¿Por qué es importante este control?

Si bien los atacantes pueden acceder a una red de muchas formas posibles, el método más común y exitoso es a través de ataques relacionados con el correo electrónico, como phishing, suplantación de identidad e interceptación. El phishing es un método de ataque en el que a los empleados se les envía un correo electrónico con un archivo, enlace o solicitud maliciosa. Si el empleado lo abre, un archivo malicioso puede cargar malware en la red del PWS, un enlace malicioso puede descargar malware o robar las credenciales del empleado, o una solicitud maliciosa puede engañar a un empleado para que comparta credenciales o fondos del PWS.

La suplantación de identidad es un método que los atacantes suelen utilizar junto con el phishing, en el que se diseña un correo electrónico malicioso para que parezca que proviene de una fuente aceptable. Este engaño se puede realizar copiando el estilo y la dirección de correo electrónico de una empresa conocida.

La interceptación es un método en el que un atacante puede colocarse entre el remitente y el receptor de un correo electrónico, lo que le da la oportunidad de robar el correo electrónico y su contenido.

Los empleados del PWS deben conocer estos métodos de ataque, pero también existen controles técnicos que pueden filtrar algunos de estos correos electrónicos maliciosos antes de que lleguen a los empleados. Este control es importante porque el uso de estos controles técnicos puede reducir el riesgo de ataques realizados mediante correos electrónicos a las operaciones del PWS.

Lineamientos adicionales

- En toda la infraestructura de correos electrónicos del PWS, habilite seguridad de la capa de transporte de inicio (STARTTLS), marco de políticas del remitente (SPF) y correo identificado de DomainKeys (DKIM). Además, habilite autenticación, informes y conformidad de mensajes del dominio (DMARC) y configúrelo en Rechazar. La CISA del DHS recomienda estos ajustes de seguridad para los correos electrónicos.

Consejos de implementación

Los PWS deben realizar campañas de capacitación y concientización de los empleados para complementar estos controles técnicos recomendados y reducir el riesgo general de ataques mediante correos electrónicos a la red del PWS.

Si bien el PWS debe evitar todas las conexiones entre la OT y la Internet pública, si es posible (consulte la hoja informativa 5.5), el PWS no debe configurar ningún activo de OT para recibir correos electrónicos, ya que los ataques por correo electrónico son comunes y, a menudo, efectivos.

Recursos

BOD 18-01 de la CISA del DHS: consulte este recurso para obtener más información sobre cómo configurar varios controles de seguridad para correos electrónicos. *https://www.cisa.gov/binding-operational-directive-18-01*

Norma 800-82 del NIST (revisión 2). Guía para la seguridad del sistema de control industrial (ICS): consulte la sección 5.8.8 (página 5-18) para obtener más información sobre el Protocolo simple de transferencia de correos (SMTP). *https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final*

NIST 800-53 (revisión 5). Controles de seguridad y privacidad para sistemas de información y organizaciones: consulte el control SI-8 (página 348) y SC-18 (página 311) para obtener más información sobre Protección contra correos no deseados y la gestión de macros, denominado Código móvil. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

APÉNDICE C: Glosario de términos

Término	Definición
Listas de control de acceso	Listas que identifican a aquellas personas que pueden acceder a un sistema de tecnología operativa (OT) o tecnología de la información (IT).
Servicios activos	Programas que se ejecutan en segundo plano.
Activo	Una instalación cibernética, dispositivo, información o proceso que tiene valor.
Bloqueo automático de cuenta o umbral de bloqueo de cuenta	Política que determina cuántas veces una persona puede intentar iniciar sesión con credenciales incorrectas antes de que el sistema la bloquee.
Servidor bastión	Una computadora con un propósito especial en una red de OT o IT que un sistema público de agua (PWS) diseña y configura específicamente para soportar ataques cibernéticos.
Copia de seguridad	El proceso de crear una copia de los datos cruciales del PWS que se pueden usar para la recuperación en caso de que los datos originales se pierdan o se corrompan.
Controles de compensación	Controles de seguridad y privacidad que implementa un PWS en lugar de los controles básicos descritos en la Publicación especial 800-53 del Instituto Nacional de Normas y Tecnología (NIST). Los controles de compensación brindan una protección equivalente o comparable para un sistema de OT o IT.
Configuración	La configuración de un sistema o componente de OT o IT, incluidas las condiciones, los parámetros y las especificaciones.
Control	Una práctica o medida que utiliza un PWS para prevenir, detectar y mitigar amenazas y ataques cibernéticos. Las prácticas van desde controles físicos, como la eliminación de puertos USB en computadoras portátiles, hasta controles técnicos, como el uso de cortafuegos y autenticación de varios factores.
Sistema de control	Un sistema que asiste en la implementación de un procedimiento o proceso (p. ej., tratamiento de agua).

Término	Definición
	Los sistemas de control incluyen control de supervisión y adquisición de datos (SCADA), sistema de control distribuido (DCS), controladores lógicos programables (PLC) y otros tipos de sistemas de control industrial.
Credenciales	Información que es exclusiva de un usuario específico y que se requiere para iniciar sesión en un sistema o programa. Por ejemplo, un nombre de usuario y una contraseña.
Prevención de pérdida de datos (DLP)	La práctica de detectar y prevenir violaciones de datos, exfiltración (robo o eliminación no autorizada o movimiento de datos de un dispositivo) o destrucción no deseada de datos confidenciales. Las organizaciones usan la DLP para proteger y asegurar sus datos y cumplir con las regulaciones.
Zona desmilitarizada (DMZ)	Una red perimetral que actúa como una cerca y controla el intercambio de información entre las redes informáticas internas y externas. Regula cómo fluye la información de una red interna a una red externa y quién desde la red externa puede acceder a la red interna. Se suele usar entre las redes de OT y IT de un PWS.
Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) del Departamento de Seguridad Nacional (DHS)	La CISA lidera el esfuerzo nacional a fin de comprender, administrar y reducir el riesgo para la infraestructura física y cibernética de la nación. La CISA desarrolla y publica una variedad de información, recursos, herramientas y capacitación para el sector del agua y otros sectores de infraestructura crítica.
Dispositivos	Piezas de hardware informático que incluyen equipos de escritorio, portátiles, servidores y tabletas.
Correo identificado de DomainKeys (DKIM)	Método de autenticación de correo electrónico para verificar la autenticidad de los correos electrónicos.
Autenticación, informes y conformidad de mensajes del dominio (DMARC)	Un protocolo que utiliza el marco de políticas del remitente (SPF) o registros DKIM para autenticar correos electrónicos. Permite el rechazo de correos electrónicos fraudulentos.
Código incrustado	Código que genera un sitio web de terceros, como YouTube o Twitter, que un usuario puede copiar y pegar en su propia página web.

Término	Definición
	Este código incrustado mostrará los mismos medios, aplicaciones o fuentes en la página web del usuario que en el sitio web original.
Plan de Respuesta a Emergencias (ERP)	Un plan que describe estrategias, recursos, planes y procedimientos que los PWS pueden usar para prepararse y responder a un incidente natural o provocado por el hombre que amenaza la vida, la propiedad o el medioambiente.
Cifrar	Proceso mediante el cual un PWS convierte texto o datos sin formato en texto o datos codificados o cifrados.
Cifrado	Cualquier procedimiento que utiliza un PWS para convertir texto o datos sin formato en texto/datos codificados o cifrados para lograr que nadie, excepto el destinatario previsto, decodifique y lea el texto o los datos.
Ejecutable	Una pieza de código de computadora o programación que puede realizar tareas establecidas de acuerdo con sus instrucciones codificadas. Un programa o rutina informática utilizan los archivos ejecutables.
Tolerancia a fallos	La capacidad de un sistema (p. ej., una computadora, una red de OT o IT, un clúster en la nube) para continuar funcionando sin interrupción cuando uno de sus componentes o más fallan.
Identidad rápida en línea (FIDO)/protocolo de cliente a autenticador (CTAP)	Desarrollado por FIDO Alliance, el CTAP permite la comunicación sin el uso de contraseñas entre un autenticador externo (p. ej., teléfonos móviles, dispositivos conectados) y otro cliente (p. ej., navegador) o plataforma (p. ej., sistema operativo como Microsoft Windows).
Centro de Denuncias de Delitos en Internet del FBI (IC3)	Una división de la Oficina Federal de Investigación que se centra en la actividad delictiva sospechosa que se presenta en Internet.
Cortafuegos	Un dispositivo que restringe la comunicación de datos entre dos redes conectadas. Un cortafuegos puede ser una aplicación instalada en una computadora de propósito general o un dispositivo separado que permite o rechaza el flujo de información entre redes.

Término	Definición
	Por lo general, un PWS utiliza cortafuegos para definir los límites de zona, como entre los sistemas de OT y IT en un PWS.
Firmware	Programa de software o instrucciones programadas en la memoria flash de solo lectura (ROM) de un dispositivo de hardware. Permite que el dispositivo se comunique con otro hardware de la computadora.
Objeto de políticas de grupo (GPO)	Permite que un administrador del sistema dicte cómo interactuarán los usuarios y las computadoras. Las políticas de grupo son principalmente herramientas de seguridad y un PWS puede usarlas para aplicar ajustes de seguridad a usuarios y computadoras, como requerir una longitud mínima de contraseña.
Interfaz entre hombre y máquina (HMI)	Interfaz de usuario o panel que conecta a un usuario con una máquina, sistema o dispositivo. El término HMI se suele usar en el contexto de un proceso industrial, como la interacción con un sistema de SCADA. Por ejemplo, un operador de PWS podría usar una HMI para verificar si una determinada bomba está funcionando.
Dirección de protocolo de Internet (IP)	Una dirección numérica que identifica un dispositivo en Internet o en una red local.
Plan de Respuesta a Incidentes (IR)	Un conjunto de procedimientos predeterminados y documentados para identificar y responder ante un incidente cibernético. Algunos PWS pueden incluir su plan de IR de seguridad cibernética como parte de su Plan de Respuesta a Emergencias del PWS.
Centros de análisis e intercambio de información (ISAC)	Una organización que recopila, analiza y difunde información factible sobre amenazas a sus miembros y les comparte herramientas para mitigar los riesgos y mejorar la resiliencia. Por ejemplo, WaterISAC brinda estos servicios a los PWS.
Sistema de información	Conjunto interconectado de recursos de información que se encuentran bajo el mismo control directo de gestión que comparten una función en común. Un sistema normalmente incluye hardware, software, información, datos, aplicaciones, comunicaciones y personas.

Término	Definición
Tecnología de la información (IT)	Conjunto de recursos que utiliza una organización para recopilar, procesar, mantener, utilizar, compartir, difundir o disponer de información.
Sistema de control industrial (ICS)	Un sistema utilizado para controlar procesos industriales como el tratamiento y la distribución de agua. Los ICS incluyen sistemas de SCADA (utilizados con frecuencia en el PWS para controlar activos dispersos geográficamente), sistemas de control distribuidos y sistemas de control más pequeños que utilizan PLC para controlar procesos localizados.
Interceptación	La interceptación permite a los atacantes acceder a datos, aplicaciones o sistemas y se trata principalmente de ataques contra la confidencialidad. Esto podría incluir ver o copiar archivos de manera no autorizada, escuchar conversaciones telefónicas o leer el correo electrónico de otra persona. Estos ataques se pueden realizar contra datos en reposo (p. ej., guardados en un servidor) o en movimiento (p. ej., un correo electrónico en tránsito del remitente al receptor).
Comisión Electrotécnica Internacional (IEC)	Una organización global de membresía sin fines de lucro que reúne a 173 países y coordina el trabajo de 20 000 expertos a nivel mundial. Facilita el acceso a la electricidad y verifica la seguridad, el rendimiento y la interoperabilidad de los dispositivos y sistemas eléctricos y electrónicos, incluidos los dispositivos de consumo como teléfonos móviles, refrigeradores, equipos médicos y de oficina, IT, generación de electricidad y mucho más.
Sociedad Internacional de Automatización (ISA)	Asociación profesional sin ánimo de lucro fundada en 1945 para crear un mundo mejor a través de la automatización. La ISA desarrolla normas globales ampliamente utilizadas, certifica profesionales, brinda educación y capacitación, publica libros y artículos técnicos, organiza conferencias y exhibiciones, y ofrece programas de establecimiento de contactos y desarrollo profesional para sus miembros y clientes en todo el mundo.
Sociedad Internacional de Automatización/Comisión	La serie de normas 62443 de la ISA/IEC, desarrollada por el comité ISA99 y adoptada por la IEC, proporciona un

Término	Definición
Electrotécnica Internacional (ISA/CEI) 62443	marco flexible para atender y mitigar las vulnerabilidades de seguridad actuales y futuras en los sistemas de control y automatización industrial (IACS).
Intranet	Una red de comunicaciones local que se suele utilizar para mejorar la comunicación, la colaboración y el compromiso dentro de una organización. Por lo general, excluye a cualquier persona ajena a la organización.
Sistema de identificación de intrusos/sistema de protección contra intrusiones (IDS/IPS)	Ambos sistemas se colocan dentro de una red para alertar cuando se produce una intrusión no deseada. Un IDS está diseñado para proporcionar solo una alerta sobre un posible incidente. Un IPS, por otro lado, actúa para bloquear el intento de intrusión o remediar el ataque.
Inventario	La lista o registro formal de la propiedad de la organización en un PWS.
Caja de salto	Un dispositivo reforzado y monitoreado que abarca dos zonas de seguridad de red distintas y proporciona un medio de acceso controlado entre ellas. Esencialmente sirve como un puente cerrado entre las zonas.
Catálogo de vulnerabilidades usadas conocidas (KEV)	Una lista de vulnerabilidades que la CISA ha identificado como usadas o que los responsables de las amenazas han utilizado para realizar ataques.
Privilegios mínimos	El principio de que una organización debe diseñar la seguridad cibernética de modo que otorgue a cada usuario los recursos mínimos del sistema y las autorizaciones necesarias para hacer su trabajo.
Registro	Un registro de los eventos que ocurren dentro de los sistemas y redes de OT y IT de un PWS.
Dirección de control de acceso a medios (MAC)	Un identificador único asignado a un controlador de interfaz de red (NIC) para su uso como dirección de red. Los fabricantes de dispositivos suelen asignar direcciones MAC, por lo que los dispositivos vienen con esta dirección ya asignada,

Término	Definición
	a diferencia de las direcciones de IP. También se conoce como dirección de hardware o dirección física.
Macro	Una acción configurada que permite a los usuarios automatizar tareas y agregar funciones en los archivos (p. ej., un botón de comando y una macro asociada en un formulario). La macro contiene los comandos que ejecutará el botón cada vez que un usuario haga clic en él.
MITRE ATT&CK	Una guía para clasificar y describir intrusiones y ataques cibernéticos.
Autenticación de varios factores (MFA)	Una función que requiere más de un factor de autenticación distinto, como un código enviado por mensaje de texto a un teléfono celular, para activar un dispositivo o iniciar sesión en una cuenta.
Base de datos de vulnerabilidad nacional (NVD)	La NVD se estableció para compartir un repositorio de datos del Gobierno de EE. UU. sobre vulnerabilidades de software y ajustes de configuración.
Segmentación de la red	Dividir una red en varios segmentos o subredes, cada uno de los cuales actúa como su pequeña red propia. Esta función permite el control del flujo de información entre subredes. Los PWS pueden usar la segmentación para mejorar el monitoreo, aumentar el rendimiento, localizar problemas técnicos y mejorar la seguridad cibernética.
Instituto Nacional de Normas y Tecnología (NIST)	Una organización que desarrolla normas, pautas, prácticas recomendadas y otros recursos de seguridad cibernética para satisfacer las necesidades de la industria estadounidense, las agencias federales y el público en general.
Marco de seguridad cibernética (CSF) del NIST	Orientación voluntaria, basada en estándares, pautas y prácticas existentes, para que organizaciones como los PWS gestionen y reduzcan mejor el riesgo de seguridad cibernética. Además de ayudar a las organizaciones a gestionar y reducir los riesgos, el NIST diseñó el CSF para fomentar las comunicaciones sobre la gestión de riesgos y seguridad cibernética entre las partes interesadas internas y externas de la organización.

Término	Definición
Conmutador de red	Un dispositivo que conecta usuarios, aplicaciones y equipos a través de una red para que puedan comunicarse entre sí y compartir recursos.
Tráfico de la red	La cantidad de datos que se mueven a través de una red durante un tiempo determinado.
Sistema operativo (SO)	Software que sirve como interfaz entre el hardware de la computadora y el usuario. Las aplicaciones (p. ej., Microsoft Office) requieren un entorno para operar y realizar tareas. El sistema operativo ayuda a los usuarios a interactuar con las aplicaciones y otro hardware y programas. El sistema operativo también realiza tareas como la gestión de archivos, memoria y procesos.
Tecnología operativa (OT)	Los componentes de hardware, software y firmware de un sistema que utiliza un PWS para detectar o generar cambios en los procesos físicos mediante la supervisión y el control directos de los dispositivos físicos. Para muchos PWS, este es un sistema de SCADA.
Parches	Actualizaciones de software y sistema operativo que abordan vulnerabilidades de seguridad dentro de un programa o producto. Los proveedores de software pueden optar por lanzar actualizaciones para corregir errores de rendimiento y proporcionar funciones de seguridad mejoradas.
Información de identificación personal (PII)	Cualquier información que permita inferir directa o indirectamente la identidad de un individuo.
Programa de Información de Infraestructura Crítica Protegida (PCII)	El Programa de PCII protege la información que habitualmente no es de dominio público y está relacionada con la seguridad de la infraestructura crítica o los sistemas protegidos, incluidos documentos, registros u otra información de las leyes de divulgación federales, estatales y locales. Esto permite a los socios, como los PWS, compartir de forma segura su información de infraestructura crítica con el DHS sin temor a la divulgación.
Phishing	Correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos que engañan a las personas para que descarguen malware, compartan información confidencial (p. ej., números del Seguro Social,

Término	Definición
	de tarjetas de crédito y de cuentas bancarias, credenciales de inicio de sesión) o realicen otras acciones que los expongan a ellos mismos o a sus PWS al delito cibernético.
Cuenta con privilegios	Una cuenta de usuario que tiene más privilegios que los usuarios normales. Las cuentas con privilegios pueden, por ejemplo, instalar o eliminar software, actualizar el sistema operativo o modificar las configuraciones del sistema o de la aplicación. Estas cuentas también pueden tener acceso a archivos a los que los usuarios estándar no pueden acceder. En un PWS, lo más probable es que un administrador del sistema tenga una cuenta privilegiada.
Controlador lógico programable (PLC)	Una pequeña computadora industrial diseñada originalmente para realizar las funciones lógicas ejecutadas por hardware eléctrico (p. ej., relés, interruptores y temporizadores o contadores mecánicos). Los PLC se han convertido en controladores con la capacidad de controlar procesos complejos, y los PWS los usan con frecuencia en sistemas de SCADA.
Arquitectura de referencia empresarial de Purdue (PERA) o modelo de Purdue	Un modelo de seis capas para la segmentación de la red de ICS que define los componentes del sistema que se encuentran en cada una de las capas y los controles de límites de la red para proteger cada capa y, en última instancia, la red del ICS.
Protocolo de acceso remoto a la computadora (RDP)	Un protocolo de comunicaciones de red desarrollado por Microsoft. Permite a los administradores del sistema diagnosticar de forma remota los problemas que encuentran los usuarios individuales y les brinda acceso remoto a las computadoras de escritorio de su trabajo físico. Los técnicos de soporte a menudo usan el RDP para diagnosticar y reparar el sistema de un usuario de forma remota.
Enrutador	Un dispositivo que se comunica entre Internet y los dispositivos en un PWS que se conectan a Internet.
Servidor	Un programa o dispositivo informático que proporciona un servicio (como compartir datos o recursos) a otro programa informático y su usuario, también conocido como el cliente.

Término	Definición
Control de supervisión y adquisición de datos (SCADA)	Un tipo de sistema de control industrial. Es una colección de elementos de software y hardware que permite a los usuarios controlar, monitorear y automatizar procesos. Los sistemas de SCADA ayudan a recopilar y analizar datos en tiempo real.
Capa de conexión segura (SSL)	Un protocolo que utiliza un PWS para proteger la información privada durante la transmisión a través de Internet.
Marco de políticas del remitente (SPF)	Un método de autenticación de correos electrónicos que ayuda a proteger el correo electrónico saliente para que las organizaciones receptoras no lo marquen como correo no deseado.
Acuerdo de nivel de servicio (SLA)	Un compromiso entre un proveedor de servicios (p. ej., vendedor) y un cliente (p. ej., el PWS). Los aspectos de calidad y disponibilidad del servicio, así como las responsabilidades individuales de las partes, se acuerdan previamente.
Suplantación de identidad	Un tipo de estafa en la que un atacante encubre una dirección de correo electrónico, un nombre para mostrar, un número de teléfono, un mensaje de texto o la URL de un sitio web para convencer a un objetivo de que está interactuando con una fuente conocida y confiable.
Seguridad de la capa de transporte de inicio (STARTTLS)	Un protocolo utilizado para garantizar que el correo electrónico se envíe de forma segura de un servidor a otro.
Ataque a la cadena de suministro	Un tipo de ataque cibernético dirigido hacia un proveedor externo de confianza que ofrece servicios o software vitales para la cadena de suministro. Los ataques a la cadena de suministro son difíciles de detectar, ya que se basan en software en el que ya se ha confiado y que puede distribuirse ampliamente (p. ej., el ataque de SolarWinds).
Administrador de sistema	Persona responsable de administrar, actualizar y operar los sistemas informáticos. Esta persona puede ser parte del PWS o un proveedor.
Control de eventos e información de seguridad (SIEM)	Una herramienta que recopila datos de registro de eventos de una variedad de fuentes (p. ej., dispositivos, software), identifica la actividad que se desvía de lo normal con análisis en tiempo real e implementa las acciones adecuadas.

Término	Definición
	Ayuda a las organizaciones a detectar, analizar, y responder a las amenazas de seguridad antes de que interrumpan las operaciones.
Ejercicio de simulación (TTX)	Un ejercicio basado en debates en el que el personal que cumple funciones y responsabilidades dentro de un plan de IR en particular se reúne en un salón de clases o en grupos de trabajo para validar el contenido del plan conversando sobre sus funciones durante una emergencia cibernética y sus respuestas a un incidente cibernético en particular. Un facilitador inicia el debate presentando un escenario y haciendo preguntas basadas en este.
Tácticas, técnicas y procedimientos (TTP)	Este es el término utilizado por los profesionales de la seguridad cibernética para describir los comportamientos, los procesos, las acciones y las estrategias utilizadas por un atacante para participar en ciberataques.
Cifrado de datos transparente (TDE)	El TDE permite al usuario cifrar datos confidenciales que se almacenan en bases de datos a nivel de archivo. Protege los datos en reposo, no los datos en tránsito.
Seguridad de la capa de transporte (TLS)	Un protocolo de autenticación y cifrado ampliamente implementado en navegadores y servidores web. El tráfico del protocolo de transferencia de hipertexto (HTTP) (un método estándar para la comunicación entre clientes y servidores web) transmitido mediante TLS se conoce como protocolo seguro de transferencia de hipertexto (HTTPS).
Red privada virtual (VPN)	Un servicio que extiende una red privada a través de una red pública (p. ej., Internet) y proporciona un canal seguro y cifrado entre el dispositivo del usuario y la red privada. Una VPN permite a los usuarios realizar el trabajo de forma remota.
Vulnerabilidad	Una falla o debilidad en una pieza de software o firmware que un atacante puede usar para modificar el código de la aplicación, dañar un activo, obtener acceso a una red o ejecutar otra actividad maliciosa.
Punto de acceso inalámbrico	Un dispositivo que crea una red de área local inalámbrica (WLAN) generalmente en una oficina o un edificio grande.

Término	Definición
	Un punto de acceso se conecta a un enrutador, conmutador o concentrador con cable y proyecta una señal wifi dentro de un área designada.