Costo: $	Impacto: ALTO	Complejidad: MEDIO

1.E: ¿Aplica el WWS parches o mitiga de algún modo las vulnerabilidades conocidas en el plazo recomendado?

Recomendación: Identifique y aplique parches a las vulnerabilidades en función de los riesgos (p. ej., primero los activos críticos) lo más rápido posible.

¿Por qué es importante este control?

Este control es importante porque reduce las posibilidades de que los atacantes aprovechen las vulnerabilidades publicadas para infiltrarse en sus sistemas informáticos.

Una vulnerabilidad es una debilidad en una parte del *software* o *firmware* que se ejecuta en un activo de *hardware*. Las vulnerabilidades pueden surgir de errores en el código o descuidos en el proceso de diseño del *software* o los atacantes pueden colocar vulnerabilidades intencionalmente en el *software* mientras un distribuidor escribe el código (es decir, un ataque a la cadena de suministro). Un *exploit* es un conjunto de acciones o un fragmento de código malicioso que los atacantes utilizan contra la vulnerabilidad, lo que les ayuda a infiltrarse en un sistema informático o dañar un activo.

El creador original del *software* proporcionará una nueva versión que no contiene la misma debilidad. Instalar esta actualización de *software* se conoce como "parchear" un sistema, y actualizarlo a la nueva versión evita que un ataque aproveche la vulnerabilidad conocida.

Consejos de implementación

Puede utilizar su inventario de activos (consulte la hoja informativa 1.A), la documentación de configuración (consulte la hoja informativa 2.O) y los recursos que se indican a continuación para identificar las vulnerabilidades que existen en su sistema. Para los activos de TI, las actualizaciones y los parches automáticos ya suelen estar habilitados (p. ej., las actualizaciones de Windows). Sin embargo, para los activos de TO, el WWS suele deshabilitar las actualizaciones y los parches automáticos. Por lo tanto, es posible que un WWS deba aplicar manualmente las actualizaciones y los parches para los activos de TO en función de la disponibilidad y la factibilidad operacional. Si un parche no está disponible o interrumpiría de forma inaceptable las operaciones de su WWS, puede utilizar controles de mitigación como la segmentación de la red (consulte la hoja informativa 2.F).

ORIENTACIÓN ADICIONAL

- En el caso de los activos en los que no es factible aplicar parches, aplique controles compensatorios, como la segmentación (es decir, separar digitalmente la red en partes más pequeñas, cada una protegida de las otras) y mejorando el monitoreo (p. ej., mediante la instalación de herramientas de monitoreo del tráfico de la red).
- Las medidas aceptables hacen que el activo sea inaccesible desde el Internet público o reducen la capacidad de los atacantes de utilizar la vulnerabilidad en un ataque informático.

El Gobierno Federal de EE. UU. mantiene varios recursos de datos sobre 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 conocidas aprovechadas (KEV) publicada por la CISA del Departamento de Seguridad Nacional (DHS), que contiene información sobre las vulnerabilidades que los atacantes ya están utilizando. Cualquier vulnerabilidad en la KEV debe recibir el mayor grado de priorización. La base de datos nacional de vulnerabilidades (NVD) publicada por el NIST contiene información sobre todas las vulnerabilidades conocidas públicamente. Su empresa de servicios públicos también debe registrarse para recibir alertas y avisos del DHS sobre nuevas vulnerabilidades. Los miembros de WaterISAC también reciben notificaciones sobre amenazas de ciberseguridad, incluyendo vulnerabilidades críticas.

Para automatizar el proceso de identificación de vulnerabilidades, la CISA del DHS ofrece servicios gratuitos para sistemas conectados a Internet (consulte la hoja informativa 2.W) y muchos distribuidores ofrecen herramientas y servicios pagos de análisis de vulnerabilidades para sistemas informáticos internos. Para ayudar a identificar vulnerabilidades, su WWS puede utilizar un análisis de vulnerabilidades en la red de TI y una herramienta de monitoreo pasivo en la red de TO del WWS.

Sistemas de TI del WWS

En el caso de la red comercial de primera línea, la gestión de parches y vulnerabilidades generalmente se puede alinear con las prácticas estándar de la red de TI, con solo excepciones limitadas. Este enfoque permite la aplicación más frecuente y rutinaria de actualizaciones y parches, típica de los entornos de TI, aprovechando los sistemas automatizados y las capacidades de implementación rápida. Sin embargo, es importante reconocer y planificar cualquier excepción específica de la red comercial que pueda requerir desviaciones de estos procedimientos estándar. La adaptación de la gestión de parches para permitir estas excepciones garantiza que se mantenga la seguridad y la eficiencia operacional sin comprometer las necesidades únicas de la red comercial. Esta alineación estratégica debe documentarse explícitamente en las políticas de ciberseguridad de la organización para proporcionar una orientación clara sobre el manejo de excepciones y al mismo tiempo cumplir con las buenas prácticas de gestión de la seguridad de la TI.

Sistemas de TO del WWS

A diferencia de los sistemas de TI, los sistemas de TO requieren enfoques personalizados debido a la dependencia de distribuidores externos y las posibles interrupciones operacionales de las actualizaciones frecuentes. Por lo tanto, se recomienda establecer ventanas de mantenimiento programadas coordinadas periódicamente con distribuidores externos, utilizando interrupciones planificadas para implementar y probar parches. Además, es fundamental contar con acuerdos de apoyo que cubran tanto las intervenciones programadas como las de emergencia, e implementar controles compensatorios para mitigar los riesgos hasta que dichas actualizaciones puedan aplicarse de forma segura. Estas prácticas deben estar vinculadas a metas estratégicas de ciberseguridad más amplias para garantizar un enfoque integral que permita mantener la integridad operacional y, al mismo tiempo, gestionar los riesgos de seguridad.

Recursos

Estándar 800-53 (revisión 5) del NIST, 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 la remediación de fallas (sección "Flaw Remediation") y el monitoreo y análisis de vulnerabilidades (sección "Vulnerability Monitoring and Scanning").
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Guía de plantillas de gestión de políticas del NIST: Consulte la sección 4.0, "Information statement" (Declaración de información) del documento sobre gestión de parches. Una plantilla que las empresas de servicios públicos pueden usar para crear una estrategia de gestión de parches.
https://www.cisecurity.org/wp-content/uploads/2020/06/Patch-Management-Standard.docx

Vulnerabilidades conocidas aprovechadas (KEV) de la CISA del DHS: Consulte este recurso para conocer las vulnerabilidades que los atacantes ya han aprovechado.
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 registrarse para recibir alertas por correo electrónico del Sistema Nacional de Concientización Informática de la CISA del DHS sobre nuevas vulnerabilidades.
https://www.cisa.gov/uscert/ncas/alerts

WaterISAC: Consulte este recurso para obtener más información sobre el Centro de Intercambio y Análisis de Información (ISAC) sobre Agua.
https://www.waterisac.org/

Principales medidas informáticas para proteger los sistemas de agua de la CISA: Consulte el punto 7 de la página 2 de este recurso para obtener información adicional.
https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems