CADENA DE CUSTODIA Y SISTEMAS DE INFRAESTRUCTURA CRÍTICA

La cadena de custodia es un proceso complejo. A menudo asociado con la preservación de pruebas para el cumplimiento de la ley, la cadena de custodia también desempeña un papel importante en la seguridad y la mitigación de riesgos para los sectores de infraestructura crítica y sus activos. Sin prácticas seguras de cadena de custodia, los actores maliciosos podrían acceder a los sistemas, activos y datos de infraestructura crítica, ya sea de manera intencional o no, y manipularlos. La integridad de los activos y sistemas de infraestructura crítica también podría ser cuestionada, sin que los propietarios y operadores de infraestructura crítica tengan la capacidad demostrar lo contrario.

Esta entrega de perspectivas CISA proporciona una descripción general de la cadena de custodia, destaca los posibles impactos y riesgos resultantes de una cadena de custodia rota o incompleta, y ofrece a los propietarios y operadores de infraestructuras críticas un marco inicial para proteger sus activos físicos y digitales.

¿QUÉ ES LA CADENA DE CUSTODIA?

La cadena de custodia es un proceso que se utiliza para rastrear el movimiento y el control de un activo a lo largo de su ciclo de vida mediante la documentación de cada persona y organización que maneja un activo, la fecha/hora en que se recolectó o transfirió y el propósito de la transferencia. Algunos ejemplos de activos incluyen equipos, infraestructura, pruebas, sistemas y datos. Mantener la cadena de custodia aumenta la transparencia y permite rendir cuentas de las acciones llevadas a cabo con el activo. En la práctica, la documentación de la cadena de custodia puede respaldar la mitigación de riesgos al reducir la oportunidad de que los actores maliciosos manipulen el activo o los datos mientras están en inactivos o en tránsito.

Ejemplos de Cadena de Custodia Física

- **Sector Químico:** Los transportadores ferroviarios de carga y los remitentes y receptores de materiales peligrosos deben implementar requisitos de cadena de custodia para garantizar un intercambio positivo y seguro de materiales peligrosos.
- **Subsector de Infraestructura Electoral**: Las prácticas de cadena de custodia para una elección incluyen formularios de control, sellos y bolsas a prueba de manipulación y equipos serializados para garantizar que las papeletas y los medios removibles que contienen datos confidenciales sean auténticos y no hayan sido comprometidos.

Ejemplos de Cadena de Custodia Digital

- **Sector Servicios de salud y Salud Pública**: Los procesos de cadena de custodia en los laboratorios certificados por el Departamento de Salud y Servicios Humanos de EE. UU. garantizan que ningún personal no autorizado manipule muestras, tenga acceso a los procesos de laboratorio o a áreas donde los registros son almacenados.
- **Sector de Servicios Financieros:** Las instituciones financieras deben cumplir con las normas de cadena de custodia para transferir datos electrónicos entre instituciones o para almacenarlos con el fin de evitar la pérdida de datos o interferencia alguna.

CADENA DE CUSTODIA ROTA

Una ruptura en la cadena de custodia se refiere a un período durante el cual el control de un activo o de datos es incierto y durante el cual las acciones realizadas sobre el activo no se han reportado o confirmado. Tales rupturas presentan oportunidades para causar daño, ya sea de manera intencional o no, que pueden comprometer la integridad del activo o los datos. En caso de que se rompa la cadena de custodia, se debe evaluar la integridad y confiabilidad del sistema, los componentes y los datos que lo acompañan del activo para determinar si pueden ser restaurados a su estado original y reinstalados en el activo.

Una ruptura en la cadena de custodia que se produce cuando una organización no validada o un actor malicioso obtiene custodia o acceso aumenta el riesgo de que no se pueda restaurar la integridad o confiabilidad del activo. Es posible que la información disponible no sea suficiente para demostrar que la confidencialidad, integridad o disponibilidad del activo no se vio comprometida.

Impactos potenciales de una cadena de custodia rota

- La integridad del sistema y sus datos subyacentes no es confiable.
- La confiabilidad, precisión y seguridad de los registros en cuestión, físicos o digitales no pueden ser garantizadas.
- Los sistemas y datos pueden ser inadmisibles en un tribunal de justicia.
- La incapacidad de proporcionar evidencia de que un sistema no se ha visto comprometido hace que no sea posible determinar si un actor malicioso (o cualquier actor) ha obtenido acceso y/o manipulado los sistemas y los datos.

PAUTAS PARA ASEGURAR LA CADENA DE CUSTODIA

Para abordar el riesgo y mejorar la seguridad y la resiliencia, los propietarios y operadores de infraestructura crítica pueden utilizar el marco de seguridad cibernética (CSF, por sus siglas en inglés) del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) para establecer estándares, pautas y normas de cadena de custodia. NIST creó el CSF, un modelo flexible, repetible, económico y enfocado en el desempeño, que consta de cinco funciones simultáneas y continuas, para mejorar la gestión de riesgos en la infraestructura crítica.
Consulte las listas a continuación para conocer los pasos prácticos para cada función de CSF.

Identificar

Desarrolle una comprensión organizacional para manejar el riesgo físico y de seguridad cibernética para sistemas, personas, activos, datos y funciones.

- Identificar los activos críticos dentro de la organización, incluyendo todos los activos utilizados para transferir datos física y digitalmente.[1]
- Hacer un inventario de todos los sistemas, dispositivos, software, datos y personas.
- Catalogar los sistemas externos, especialmente los sistemas y/o procesos dependientes con los cuales los activos críticos de la organización pueden integrarse, especialmente si esos sistemas o procesos están fuera del control de la organización.
- Documentar los formularios o registros digitales y analógicos que rastrean las transacciones y el acceso.
- Evaluar rutinariamente los registros y formularios para comprender si hay brechas en las transacciones o el acceso que pudieran conducir a una ruptura en la cadena de custodia.
- Evaluar las reglas de conservación para determinar si satisfacen las necesidades comerciales de la organización.

Proteger

Desarrollar e implementar una cadena de custodia y salvaguardas adecuadas para garantizar que los servicios, sistemas y datos críticos estén debidamente protegidos mientras están en reposo y en tránsito. Las medidas de protección mantienen alejados a los actores no autorizados y malintencionados.

- Implementar controles de acceso, tanto físicos como electrónicos, a los activos e instalaciones.
- Garantizar que las personas solo estén autorizadas a acceder a los sistemas, datos e instalaciones que son esenciales para sus funciones laborales: uso del Principio de Privilegio Mínimo.
- Asegurarse de que la integridad de la red esté protegida y de que se administre el acceso remoto.
- Implementar el monitoreo continuo de transacciones, actividades y procesos de control de acceso.
- Administrar la información y los registros de acuerdo con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.

[1] De conformidad con la Orden Ejecutiva (EO) 14028 sobre la Mejora de la Ciberseguridad de la Nación, emitida el 12 de mayo de 2021, el Instituto Nacional de Estándares y Tecnología (NIST) publicó una definición del término "software crítico". Disponible: nist.gov/itl/executive-order-improving-nations-cybersecurity/ critical-software-definition

Detectar

Desarrollar e implementar actividades apropiadas para identificar cuando una violación a la cadena de custodia tenga lugar. Las medidas de detección proporcionan evidencia de que se ha producido una infracción.

- Registrar todas las transacciones electrónicamente (por ejemplo, registros de auditoría o eventos) o físicamente a través de documentos de cadena de custodia.
- Realizar un seguimiento de cada activo de forma independiente mediante la identificación única de cada activo, como la evidencia de manipulación o la serialización.
- Establecer umbrales de alerta de incidentes.
- Garantizar el monitoreo continuo y/o alerta de las medidas de detección. Si la cadena de custodia se rompe sin haber establecido medidas de seguimiento, un incidente puede pasar desapercibido.

Responder

Desarrollar actividades apropiadas para implementar en respuesta a una violación detectada de la cadena de custodia. Las medidas de respuesta permiten a la organización determinar el impacto y las consecuencias de la infracción.

- Establecer procesos para recibir, analizar y responder a una infracción, pérdida de integridad o preservación de los registros de la cadena de custodia.
- Investigar las notificaciones de los sistemas de detección.
- Determinar si el impacto de la infracción da lugar a un incidente que deba ser notificado.
- Reportar incidentes de acuerdo con los criterios establecidos.
- Asegurarse de que el personal conozca sus derechos y el orden de las operaciones cuando se requiera una respuesta.
- Proporcionar una supervisión estricta de las actividades forenses que se realizan, incluyendo la validación del personal con el fin de garantizar la cadena de custodia y la integridad de los sistemas, los datos y cualquier evidencia recopilada.

Recuperar

Desarrollar e implementar actividades apropiadas para mantener planes de resiliencia y restaurar cualquier servicio, sistema o dato crítico que se haya visto afectado debido a la violación de la cadena de custodia o al incidente de seguridad cibernetica.

- Ejecutar procesos y procedimientos de recuperación para asegurar la restauración de los sistemas o activos afectados por el incidente.
- Limpiar los medios de acuerdo con la Publicación Especial NIST 800-88, Revisión 1.
- Revisar y evaluar el hardware para determinar si los componentes del sistema han sido reemplazados o modificados de alguna manera.
- Restaurar los sistemas utilizando una versión de validación del firmware y el software (por ejemplo, una estructura confiable).
- En los casos en que se requiera que los sistemas de infraestructura crítica deban someterse a la certificación, es posible que el organismo de certificación acreditado deba revisar los sistemas afectados para la recertificación.
- Si los sistemas o datos deben entregarse a una entidad validada, deben existir procesos para reasumir y validar la cadena de custodia antes de reintegrar esos sistemas o datos en su infraestructura. Estos procesos deberían incluir potencialmente la limpieza de medios, la instalación de estructuras confiables, la recertificación del sistema, los protocolos de pruebas de aceptación, etc.
- Puede haber situaciones en las que no sea posible restablecer la cadena de custodia o la integridad de los sistemas o datos (por ejemplo, pérdida de la cadena de custodia). En esos casos, considere la posibilidad de desmantelar y reemplazar los activos de interés.
- Puede haber situaciones en las que el tiempo, el costo y/o la experiencia para recuperar, restablecer la cadena de custodia y, potencialmente, recertificar los sistemas no sean prácticos. Un plan de recuperación debe incluir procedimientos sobre cómo manejar tal escenario, incluyendo el reemplazo total de los activos.

AUDITE SUS PROCESOS

Los propietarios y operadores de infraestructuras críticas deben auditar de forma rutinaria los procesos de la cadena de custodia para demostrar que la autenticidad de los datos recopilados se ha mantenido en todas las etapas. Las auditorías deben buscar evidencia que demuestre la efectividad y durabilidad de los procedimientos, procesos, sistemas y capacitación. La prueba de los procesos de cadena de custodia también brinda a los propietarios y operadores la oportunidad de asegurarse de que no haya brechas en el proceso de la cadena de custodia y que exista evidencia suficiente para mantener un rastro defendible de los datos recopilados en caso de un litigio o investigación.

RECURSOS

Definición de Software Crítico Bajo la Orden Ejecutiva (EO) 14028: nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition

Organización Internacional de Normalización, ISO 22095:2020 Cadena de Custodia – Terminología General y Modelos: iso.org/standard/72532.html?browse=tc

Instituto Nacional de Estándares y Tecnología, Pautas para mejorar la seguridad cibernética de las infraestructuras críticas: nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Instituto Nacional de Estándares y Tecnología, Publicación Especial 800-161 Prácticas de Gestión de Riesgos de la Cadena de Suministro para Sistemas y Organizaciones Federales de Información: doi.org/10.6028/NIST.SP.800-161r1

Publicación especial 800-88 del Instituto Nacional de Estándares y Tecnología, revisión 1, Pautas para la limpieza de medios: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf