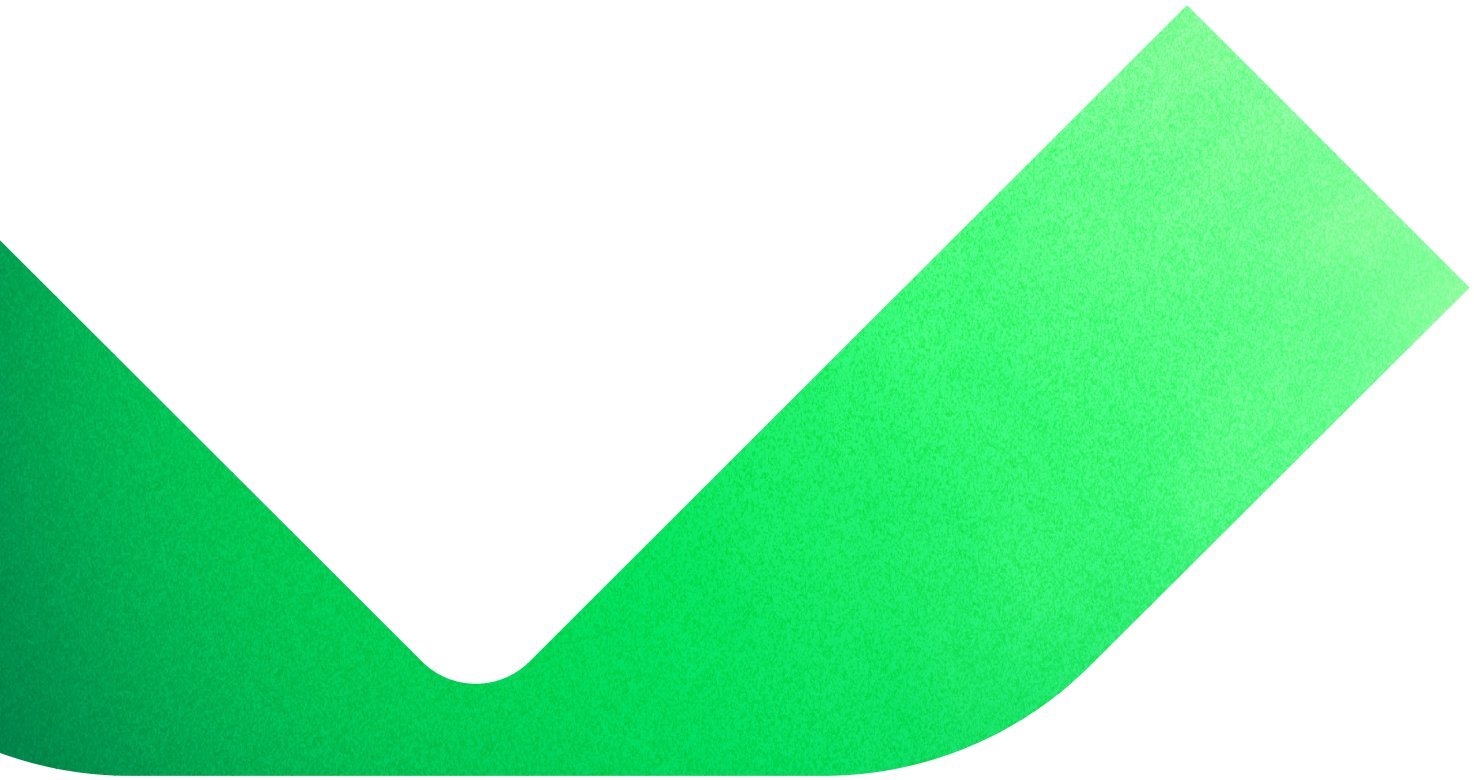
Crear una estrategia de recuperación de datos ciberresiliente



Contenido

Introducción

En el mundo donde lo digital es prioritario, la ciberseguridad es una necesidad fundamental. No es de extrañar que todos los blogs o documentos de ciberseguridad que lea hoy giren inevitablemente en torno al ransomware. Es tedioso escuchar sobre esto (¡lo sabemos!), pero el ransomware se ha convertido en la mayor amenaza para las organizaciones de todos los tamaños y apunta a nuestras infraestructuras más críticas y sectores industriales. Es un juego del gato y el ratón, y a medida que surgen nuevas amenazas, los equipos de seguridad deben adaptarse para mantenerse al día. La digitalización generalizada de las operaciones comerciales, las funciones gubernamentales y las actividades personales ha aumentado exponencialmente el volumen de datos confidenciales que se almacenan y transmiten en línea. Desafortunadamente, este cambio también ha ampliado la superficie de ataque para los ciberdelincuentes, lo que hace que las medidas de ciberseguridad sólidas sean esenciales.

Las amenazas cibernéticas, que van desde infracciones de datos y ataques de ransomware hasta sofisticados ciberespionajes patrocinados por el estado, plantean riesgos significativos para la integridad de la infraestructura crítica, la privacidad de su información personal e incluso la estabilidad de las economías globales. Por lo tanto, la seguridad de los datos debe estar a la vanguardia de la estrategia de cada organización, ya que la amenaza de los ciberataques, principalmente el ransomware, es un peligro claro y presente. Desgraciadamente, el 85 % de las organizaciones ha sufrido al menos un ataque de ransomware en 2022[1]. Lo que es aún más alarmante es el hecho de que los ataques de ransomware de hoy en día no solo bloquean a las organizaciones de sus datos, sino que los filtran, roban, venden o archivan para usarlos en otros esquemas de extorsión.

El principal objetivo de cualquier plan de ciberseguridad debería ser impedir el acceso malintencionado a estos datos. Sin embargo, ninguna organización debería contar con que sus defensas resistirán siempre. Por lo tanto, tener la capacidad de recuperar sus datos es igualmente importante. De las organizaciones afectadas por ransomware, el 15% de los datos de producción se perdió en promedio[2] , lo que resalta la importancia de tener un plan de recuperación de datos bien diseñado y confiable.

Las prácticas de ciberseguridad eficaces protegen contra el acceso no autorizado a los datos, garantizan la continuidad de las operaciones y mantienen la confianza entre los consumidores y los proveedores de servicios. A medida que las amenazas cibernéticas evolucionan en complejidad y escala, no se puede exagerar la importancia de la ciberseguridad para salvaguardar los activos digitales, proteger la privacidad individual y preservar la seguridad nacional. Es un pilar fundamental en la arquitectura de nuestra sociedad digital y garantiza que podamos navegar, innovar y comunicarnos en este ámbito con confianza.

La reciente actualización del Marco de Ciberseguridad (CSF) 2.0 del NIST[3] marca una evolución fundamental en el enfoque estándar de la ciberseguridad y refleja el cambio de paradigmas en un mundo donde las amenazas digitales son cada vez más complejas y omnipresentes.

Este documento explora el Marco CSF del NIST actualizado y analiza los lugares en los que Veeam Software puede ayudar a implementar este marco.

[1] https://go.veeam.com/wp-data-protection-trends-2024

[2] https://go.veeam.com/wp-data-protection-trends-2024

[3] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Antecedentes del Marco de Ciberseguridad del NIST

El Marco de Ciberseguridad del NIST (CSF) se introdujo por primera vez en 2014 como respuesta a la creciente necesidad de un enfoque unificado para gestionar los riesgos en materia de ciberseguridad. El Framework fue desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) a través de la colaboración con entidades del sector privado y del sector público, y su objetivo era proporcionar a las organizaciones un conjunto de estándares de la industria para ayudar a proteger sus sistemas de información. Los objetivos del CSF eran ayudar a las organizaciones a comprender y mejorar la gestión del riesgo de ciberseguridad, lo que también mejoraría la seguridad y la resiliencia de las infraestructuras críticas.

El NIST Cybersecurity framework (CSF) 2.0, publicado en febrero de 2024, se basa en versiones anteriores y aporta varios cambios significativos que reflejan la evolución del panorama de la ciberseguridad y los comentarios recibidos de la comunidad.

CSF 2.0 extiende su alcance más allá de los sectores de infraestructura crítica; se ha revisado para beneficiar a todas las organizaciones, independientemente de su tamaño o tipo, lo que hace que esta directriz sea más universalmente aplicable.

Figura 1 — NIST Cybersecurity Framework 2.0

El núcleo del CSF se organiza en torno a seis funciones principales y, cuando se consideran en conjunto, estas características crean una recomendación integral basada en el ciclo de vida de los riesgos de ciberseguridad.

- **Identificar:** Adquiera un conocimiento organizativo que le permita gestionar los riesgos de ciberseguridad para sistemas, personas, activos, datos y capacidades. Esto incluye la identificación de los procesos críticos del negocio y los activos clave, junto con sus vulnerabilidades y amenazas.
- **Proteger:** Implemente las medidas de seguridad adecuadas para garantizar la prestación de servicios críticos y limitar o contener el impacto de posibles incidentes de ciberseguridad. Esto incluye la gestión de identidades, control de acceso, seguridad de datos y tecnología de protección.
- **Detectar:** Implementar medidas para identificar oportunamente la ocurrencia de incidentes de ciberseguridad. La monitorización continua y la detección de amenazas son capacidades clave de esta función.
- **Responder:** Tome medidas cuando se detecte un incidente de ciberseguridad. Esto incluye planificación de las respuestas a incidentes, análisis, mitigación y comunicación.
- **Recuperar:** Mantenga planes de resiliencia y restauración de funcionalidades o servicios que se hayan visto afectados por un incidente de ciberseguridad. La recuperación oportuna a las operaciones normales es el objetivo.
- **Gobernar (nuevo):** Esta nueva función del CSF 2.0 se centra en la gestión general y la gobernanza del riesgo de ciberseguridad. Aquí, las organizaciones establecen su supervisión, estrategia y políticas de gestión de riesgos de ciberseguridad, incluida la definición de roles y responsabilidades y la integración de la ciberseguridad en la gestión de riesgos empresarial.

La nueva función "Gobernar" eleva los objetivos fundamentales de rendición de cuentas y transparencia y sirve como fuerza unificadora para ayudar a las organizaciones a establecer prioridades y lograr los objetivo esbozados en las otras cinco funciones. También hace hincapié en que la ciberseguridad no es una preocupación independiente, sino una parte integral de lo que constituye el riesgo empresarial. El componente de supervisión de la nueva función, en particular, ayuda a las organizaciones a cumplir con los marcos regulatorios, como las regulaciones de la SEC, que enfatizan una mayor responsabilidad para la alta gerencia y la Junta Directiva al tomar decisiones sobre la seguridad de TI.

Para mejorar la claridad y la relevancia, las cinco funciones originales: Identificar, Proteger, Detectar, Responder y Recuperar, se han conservado y actualizado para reflejar la evolución de las amenazas y prácticas de ciberseguridad, garantizando así que las organizaciones puedan gestionar y reducir eficazmente sus riesgos de ciberseguridad en un entorno digital dinámico. Los elementos relacionados con la gobernanza tambiénse han transferido a la función "Gobernar", de reciente creación. Además, los objetivos principales de cada función ahora se establecen con mayor claridad. Al reconocer que estas tareas no son partes secuenciales, sino más bien interdependientes de una estrategia de ciberseguridad global, esta reestructuración busca permitir un enfoque más cohesivo y vinculado de la ciberseguridad.

El enfoque en la gestión de riesgos de la cadena de suministro de ciberseguridad también es ahora más pronunciado, con nuevos controles destinados a integrar la gestión de riesgos de la cadena de suministro en todo el programa de ciberseguridad de una organización.

Los usuarios de este marco ahora reciben ejemplos[4] y guías de inicio rápido[5] que también se adaptan a sus necesidades específicas. Esto incluye un catálogo de referencias[6], al que se puede acceder a través de la herramienta de referencia, que permite a las organizaciones asignar orientación a más de 50 otros documentos de ciberseguridad relevantes.

[4] https://www.nist.gov/document/csf-20-implementations-pdf

[5] https://www.nist.gov/quick-start-guides

[6] https://csrc.nist.gov/projects/olir/informative-reference-catalog#

Los cambios clave incluyen:

1. CSF 2.0 extiende su aplicabilidad más allá de los sectores de infraestructura crítica. El marco modificado se ha diseñado para beneficiar a todas las organizaciones, independientemente de su tamaño o industria, al hacer que las directrices sean más pertinentes para todo el mundo.
2. La función "Gobernar" añadida es una mejora significativa de CSF 2.0. Esta función eleva los objetivos básicos de rendición de cuentas y transparencia, al tiempo que sirve como una fuerza unificadora para ayudar a las organizaciones a priorizar y alcanzar las metas descritas en las otras cinco funciones. Hace hincapié en la integración de la ciberseguridad en la gestión general de riesgos de la empresa, en lugar de considerarla como una preocupación independiente. El componente de supervisión de la función "Govern" es particularmente útil para las organizaciones en el cumplimiento de los marcos regulatorios, como las regulaciones de la SEC, que enfatizan una mayor responsabilidad para la Junta Directiva y la alta gerencia al tomar decisiones relacionadas con la ciberseguridad.
3. Un mayor enfoque en la gestión de riesgos de la cadena de suministro. CSF 2.0 pone un mayor énfasis en la gestión de los riesgos de ciberseguridad en la cadena de suministro. También se han introducido nuevos controles para integrar la gestión de riesgos de la cadena de suministro en todo el programa de ciberseguridad de una organización. Esto reconoce la importancia de proteger todo su ecosistema de socios, vendedores y proveedores de servicios.

Estas mejoras dentro de NIST CSF 2.0 proporcionan a las organizaciones un framework más completo y adaptable para ayudarlas a navegar por el complejo panorama de la ciberseguridad. Al ampliar el alcance, introducir la función "Gobernar", actualizar las funciones básicas y hacer hincapié en la gestión de riesgos de la cadena de suministro, CSF 2.0 equipa a las organizaciones con las herramientas y la orientación que necesitan para fortalecer su postura de ciberseguridad y desarrollar resiliencia frente a las amenazas en evolución.

Los usuarios de este marco ahora reciben también ejemplos[7] y guías de inicio rápido[8] que también se adaptan a sus necesidades específicas. Esto incluye un catálogo de referencias[9], al que se puede acceder a través de la herramienta de referencia, que permite a las organizaciones ofrecer orientación sobre otros 50 documentos de seguridad relevantes.

[7] https://www.nist.gov/document/csf-20-implementations-pdf

[8] https://www.nist.gov/quick-start-guides

[9] https://csrc.nist.gov/projects/olir/informative-reference-catalog#

Una base fiable para la recuperación de datos

Dentro de una estrategia de disponibilidad de datos, la recuperación de los datos suele ser la última parada de un plan de ciberseguridad, y por ello debe estudiarse y planificarse adecuadamente. La aplicación de conceptos como una estrategia de protección de los datos 3-2-1-1-0 y contar con una única herramienta que sea capaz de respaldar los datos de toda su infraestructura y restaurarlos a un estado saludable tras un incidente de ciberseguridad, proporcionará a las organizaciones la posibilidad de recuperar los datos en cualquier situación.

Figura 2 — Regla de backup 3-2-1-1-0 de Veeam

Los clientes de Veeam pueden alcanzar este objetivo de una forma segura, orquestada y bien documentada gracias a Veeam Data Platform. Utilizando la suite completa que incluye Veeam Backup & Replication, Veeam ONE y Veeam Recovery Orchestrator, los clientes de Veeam son capaces de alcanzar objetivos de seguridad de datos que están en sintonía con todas las etapas del Marco de Ciberseguridad del NIST y que van mucho más allá de la mera copia de seguridad y recuperación de datos.

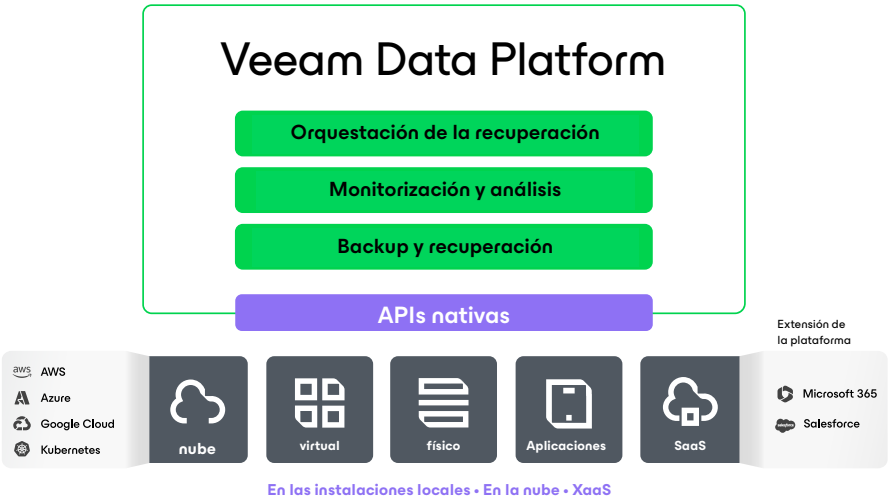


Figura 3 — Veeam Data Platform

El resto de este documento se basa en gran medida en el Framework de ciberseguridad del NIST cubierto anteriormente, y está destinado a proporcionar a las organizaciones de TI, equipos de seguridad y responsables de la toma de decisiones la información y el conocimiento que necesitan para utilizar eficazmente Veeam Plataforma de datos dentro del Framework. También queremos proporcionarle otra fuente de información y funcionalidades que le ayudarán a identificar datos críticos, detectar malware, proteger datos, responder rápidamente a amenazas activas y recuperar rápidamente datos limpios, destacando al mismo tiempo las funcionalidades clave que pueden utilizarse para lograr estos objetivos.

Función NIST "Identificar" (ID)

Resultado deseado en materia de ciberseguridad:

Conocimiento de los riesgos de ciberseguridad actuales de la organización.

La ciberseguridad comparte un mantra fundamental con la recuperación ante desastres (DR) tradicional: **Nopuedes proteger lo que no conoces.** Clasificar y categorizar los activos que necesitan protección puede parecer una tarea intrascendente si se compara con combatir y reaccionar activamente ante una amenaza de ciberseguridad, pero el primer paso que debe darse es el de saber qué está en riesgo y cuál es su prioridad relativa. Con las siguientes funcionalidades, Veeam puede convertirse en una parte instrumental de una estrategia de múltiples capas para **identificar** datos críticos.

Clasificar los sistemas y datos críticos

Para crear un plan de recuperación confiable, los departamentos de TI y seguridad deben trabajar estrechamente con la empresa a fin de identificar, clasificar y priorizar todas las cargas de trabajo y los datos que existen en toda la organización. Un excelente punto de partida para esto son los propios informes de Veeam ONE y el catálogo de sistemas cuentan con el respaldo de Veeam Backup & Replication. Debe hacerse un backup de todos los datos críticos, y Veeam permite revelar si existen máquinas virtuales o datos que no se están protegiendo.

Del mismo modo, las herramientas de red y seguridad utilizadas por el equipo de seguridad pueden crear una lista de sistemas en su entorno. La comparación de estos diversos sistemas a menudo descubrirá dónde sus datos no están protegidos adecuadamente dentro de cada una de las herramientas, lo que garantiza que sus planes de protección y recuperación sean lo más completos posible.

Identificación y priorización de los datos mediante el etiquetado y clasificación

Haciendo uso de las funcionalidades de etiquetado y clasificación de datos de Veeam Backup & Replication, los clientes pueden comenzar con un catálogo actual de cargas de trabajo (sus backups) y empezar a aplicar etiquetas para identificar metadatos del sistema como la ubicación, propietario y prioridad de recuperación.Este ejercicio, a veces, resaltará los datos que faltan, indicará una brecha en la protección de datos e identificará los metadatos clave necesarios para planificar adecuadamente la recuperación de datos.

Una vez aplicados los metadatos, se puede utilizar la planificación de recuperación basada en asistentes dentro de Veeam Recovery Orchestrator para crear el plan de recuperación, lo que reduce el tiempo necesario para su desarrollo. A continuación, puede revisarse el plan con el negocio como una comprobación más para garantizar su precisión e integridad en relación con las necesidades de la empresa.

Detectar deficiencias y cambios mediante pruebas de recuperación automatizadas

La mejor manera de identificar si un backup o plan estará listo para su uso en caso de emergencia es probarlo. Las funciones de automatización de pruebas de Veeam Recovery Orchestrator ofrecen una ventaja sustancial ya que garantizan la absoluta recuperabilidad de parte o toda la infraestructura. Además de los beneficios obvios de la reducción de mano de obra durante la ejecución de la prueba, la automatización del proceso de recuperación de la prueba también puede significar pruebas más frecuentes, lo que permite que las fallas se resalten más rápidamente.

Una de las fallas que se pueden identificar a través de pruebas frecuentes es cuando no se está haciendo backup de los sistemas o se han dejado de lado. La revisión periódica de los resultados de estas pruebas y la corrección de cualquier deficiencia mejorará el conocimiento de la organización sobre lo que necesita protección.

Función NIST "Proteger" (PR)

Resultado deseado en materia de ciberseguridad:

Implemente protecciones para garantizar la seguridad de sus activos.

La infraestructura de backup es un lugar especial para cualquier entorno de TI. No solo constituye la red de seguridad final de la seguridad de los datos, sino que también contiene múltiples copias de todos sus datos (cuanto más críticos, más copias), incluidos los datos que pueden haberse eliminado en la producción. Esto lo convierte en un objetivo principal para que los delincuentes roben sus datos y comprometan su seguridad para que sus esquemas de rescate y extorsión tengan más éxito. Por eso es fundamental que **proteja** la propia infraestructura de backup.

Una infraestructura de backup que no confía en nadie

El primer paso para proteger los backups es impedir el acceso no autorizado al propio sistema de gestión de backup. Deberían aplicarse los principios de confianza cero (verificar explícitamente, asumir la vulneración y usar el acceso con menos privilegios) para dificultar al máximo el movimiento lateral hacia su infraestructura de backup.

Utilizar la autenticación multifactor (MFA) y contar con un sistema de administración de identidad y acceso (IAM) de protección de datos independiente y dedicado garantizará que sus usuarios y sus credenciales estén debidamente verificados y sean más difíciles de comprometer. Implementar el acceso de privilegios mínimos, como tener cuentas de administrador y operativas independientes, también evitará errores involuntarios y minimizará el escalado de privilegios. Finalmente, todo debe configurarse asumiendo que el resto de su infraestructura ya se ha visto comprometida. Esto significa aislar los componentes de backup en una red separada y restringir el acceso a la consola de Veeam Backup & Replication a través de una conexión VPN o remota.

Cada nivel de su Infraestructura de backup debería incorporar estos enfoques, pero pueden ser ligeramente diferentes en cada nivel. Esto significa que los sistemas operativos, los archivos compartidos, la administración fuera de banda y cualquier aplicación utilizada para administrarlos deben seguir principios similares.

Analizar el estado de cumplimiento de la infraestructura de backup

Para ayudar a los clientes a aplicar de manera adecuada los principios Zero Trust, la consola de Veeam Backup & Replication integra una utilidad denominada "Security & Compliance Analyzer" (anteriormente conocida como Best Practices Analyzer) que analiza la infraestructura de Veeam e informa sobre los elementos de configuración que no se han implementado siguiendo nuestras recomendaciones. Este análisis debe ejecutarse de forma periódica y cada uno de los elementos no conformes debe corregirse o suprimirse. Los elementos suprimidos se anotarán junto con el usuario y la fecha y hora de la supresión. Una vez completadas las correcciones, el análisis debería ejecutarse nuevamente y documentarse los resultados.

Garantizar la disponibilidad de backups cuando se necesiten

Eliminar los archivos de backup de forma que sus datos no puedan recuperarse es ahora una de las características típicas del ransomware. Por ello es fundamental garantizar que sus backups no puedan ni modificarse ni eliminarse.

La inmutabilidad es un concepto muy antiguo en informática que recientemente se ha convertido en una característica crítica para los backups, especialmente para aquellos que necesitan conservarse sin cambios o errores para satisfacer los requisitos de retención. Tanto si utiliza repositorios reforzados, almacenamiento de objetos, dispositivo de desduplicación o cinta, los backups de Veeam pueden almacenarse en un estado tal que ni siquiera los administradores puedan modificar o eliminar los datos. Como con cualquier sistema de seguridad, a menudo existen soluciones alternativas, por lo que es fundamental considerar toda su pila, desde el piso del centro de datos, para garantizar que estas soluciones alternativas se eliminen o se controlen estrictamente.

Es un viejo chiste en ciberseguridad que el sistema más seguro es el que está apagado, desconectado de la red y almacenado en una habitación a la que nadie puede acceder. Si bien el chiste es completamente cierto, la verdad es que un sistema inaccesible no tiene razón de ser. Este dicho, sin embargo, puede funcionar bien cuando se considera la seguridad de backup. Siempre y cuando sea accesible, cuando sea necesario, una copia de backup que se almacena desconectada (offline) es la que menos probabilidad tiene de ser manipulada. Veeam ofrece varias opciones para crear este enfoque de almacenamiento aislado (air-gapped) para el backup, que va desde los sistemas en línea que requieren de una autenticación diferente, hasta el almacenamiento offline definitivo: la cinta.

Dicho esto, ningún plan debería depender únicamente de una sola capa de protección. Por lo tanto, Veeam Backup & Replication habilita un principio de "cuatro ojos" para la eliminación de backups. Emulando el conocido y antiguo enfoque del maletín del presidente con las "llaves nucleares", esta configuración requiere que dos administradores autoricen la eliminación de la copia de seguridad, protegiendo de esta forma los backups frente a un borrado accidental o malintencionado.

Cifre sus propios backups

Para proteger sus datos de un uso indebido tras una fuga de información o exfiltración, Veeam puede cifrar los backups para evitar que alguien pueda acceder a ellos fuera de su infrastructura de Veeam. Si bien esto no evitará que sus datos sean robados o bloqueados a través del ransomware, hará que sea muy improbable que sus datos sean utilizados como una vía para esquemas de extorsión. Este cifrado puede gestionarse directamente de manera interna en Veeam o vincularse a un sistema de gestión de claves (KMS) de un tercero para delegar y centralizar la gestión de dichas claves.

Barra lateral: Modelo de seguridad Zero Trust

El objetivo de Zero Trust es eliminar la confianza intrínseca que tradicionalmente ha existido dentro de la seguridad perimetral, reduciendo así la capacidad de las amenazas para moverse fácilmente a través de su entorno. Aplicando el mantra “nunca confíes, verifica siempre”, se genera un modelo de seguridad sin perímetro que no presupone que su cortafuegos se encargará de detener las ciberamenazas. En este modelo, cada sistema debe verificar cada nueva interacción y no asumir que están seguros. Los tres principios del modelo de seguridad de confianza cero son:

1. **Verifique explícitamente.**

2. **Proporcione acceso con privilegios mínimos.**

3. **Asuma la vulnerabilidad.**

Función NIST "Detectar"

Resultado deseado en materia de ciberseguridad:

Desarrollar e implementar las medidas adecuadas para identificar un evento de ciberseguridad.

Una vez que se ha identificado todo el panorama de sistemas y datos, su organización debe establecer planes y sistemas para la detección rápida de intrusiones en esos activos. Una detección rápida reducirá drásticamente el tiempo de permanencia y el impacto de la amenaza, que generalmente puede traducirse en pérdidas de dinero. En este caso, Veeam puede ser también un componente clave dentro de una estrategia multicapa para **detectar** ciberamenazas.

Poner de relieve comportamientos anómalos

Una de las estrategias clave del malware es evitar la detección mientras se escalan privilegios y se mueven lateralmente dentro del entorno, infectando así tantos sistemas como sea posible. Para lograr esto, es posible que el malware solo realice pequeños cambios a la vez para evadir su atención. Además, dado que los ciberdelincuentes se han vuelto más inteligentes para frustrar nuestros intentos de recuperar los datos por los que pedirán un rescate, estos han empezado a eliminar los backups, reducir los tiempos de retención de dichos backups o desactivar los trabajos de backup. Veeam puede identificar y alertarlo sobre estos tipos de comportamiento anómalos a través de varias alarmas e informes dentro de Veeam ONE.

Buscar malware durante el backup

Veeam Backup & Replication puede, mediante la detección de malware en línea, analizar los bloques a medida que llegan a través de los nodos del Veeam Proxy en busca de signos de un posible cifrado, el cual es uno de los indicadores clave de un malware activo. Basándose en una búsqueda en el índice backup, se detectarán nombres de archivos maliciosos y firmas, y si se encuentra algo sospechoso, el backup se marcará como sospechoso.

Detectar malware en los backups

La función SureBackup de Veeam Backup & Replication se diseñó en principio para automatizar la restauración y validación de los backups para asegurarse de que sean restaurables. Puesto que el software de protección de los endpoints no es perfecto, y podría provocar la entrada de malware en sus backups, SureBackup cuenta además con un sólido conjunto de funciones para comprobar la existencia de malware en los archivos de backup.

Como parte de una prueba de restauración, SureBackup también puede trabajar con herramientas de análisis de malware para analizar su máquina virtual restaurada (VM). Esto permite a las organizaciones usar una herramienta secundaria de detección de malware con un enfoque de tipo "confiar pero verificar". Como ventaja añadida, el análisis de SureBackup no afecta a la carga de trabajo de producción, lo que permite llevar a cabo un análisis más exhaustivo. SureBackup también puede montar discos individuales en una máquina de prueba que puede después analizar los archivos en busca de malware y, por tanto, proporcionar un análisis de malware más rápido y eficiente cuando no es necesario realizar una restauración completa.

Si se encuentra algo en estos análisis, ese punto de restauración en particular se marcará como sospechoso.

Realizar periódicamente pruebas del plan de recuperación para detectar situaciones de riesgo

Una vez más, las pruebas regulares del plan de recuperación pueden ser útiles, ya que pueden revelar la corrupción causada por el malware. Los fallos producidos durante una prueba completa del plan de recuperación, incluida la verificación de las aplicaciones, podrían llamar la atención sobre las áreas en las que se ha cifrado un archivo clave o se ha modificado de manera indebida un archivo de configuración. Esto podría ser especialmente útil para detectar malware que se ejecuta durante una secuencia de arranque.

Correlación e informe de logs centralizados

El envío de archivos de registro (logs) a un servicio syslog externo proporciona un repositorio secundario de logs y una centralización que permite la correlación de eventos entre sistemas. Esta es la función principal de un sistema de gestión de eventos e incidentes de seguridad (SIEM - Security Incident and Events Manager) para la mayoría de los equipos de seguridad. Al configurar el sistema SIEM como un destino syslog, los indicadores de compromiso descubiertos por Veeam pueden marcarse directamente en el sistema, reduciendo así el tiempo de respuesta y brindando a los analistas de seguridad una visión más sólida de un evento.

Integraciones externas para la protección de datos

La API de incidentes (Incident API) es un conjunto de interfaces de programación de aplicaciones (API) que pueden usar las herramientas de ciberseguridad para informar a la infraestructura de backup de una infección descubierta y señalar los backups como sospechosos o infectados. Veeam Backup & Recovery puede configurarse para alertar a los administradores en base a esta información, lo que les permite revisar, verificar y responder rápidamente con acciones como la creación inmediata de un backup, la ejecución de una acción SureBackup para comprobar si existe una infección y recuperar archivos limpios, y la creación de una copia inmutable de un backup con fines de análisis forense. Este punto abierto de integración entre las herramientas centrales de seguridad y su plataforma de protección de datos mejora significativamente la comunicación, y como resultado reduce el tiempo de permanencia del malware que conducirá a una recuperación más limpia y rápida.

Barra lateral: Tiempo de permanencia

El tiempo de permanencia (la cantidad de tiempo que el malware existe en el entorno antes de ser descubierto) es cuando el malware se encuentra dentro de su entorno sin ejecutar el ataque principal. Puede pasar este tiempo comprometiendo cuentas adicionales, escalando privilegios, incrustándose más profundamente en su sistema operativo, extendiéndose lateralmente a otros sistemas y recopilando inteligencia que puede utilizar para ataques actuales o futuros.

Función NIST "Responder"

Resultado deseado en materia de ciberseguridad:

Desarrolle e implemente respuestas adecuadas para la detección de un incidente de ciberseguridad.

Es imposible estar siempre completamente protegido, y por ello necesita centrarse también en detener el malware y eliminarlo lo antes posible. Al igual que la planificación de la recuperación de un desastre natural, uno de los objetivos principales con el que deben alinearse todas sus decisiones son los objetivos de tiempo de recuperación (RTO). En un incidente de ciberseguridad, existe un objetivo muy similar que se centra en detener y eliminar el malware del entorno para que se pueda volver a poner en funcionamiento los sistemas. Ser capaz de reducir el tiempo que el malware tendrá para permanecer y extraer sus datos reducirá el esfuerzo de limpieza y mejorará el tiempo de recuperación, por lo que es fundamental prepararse para responder **rápidamente** .

Uso de backups para el análisis ciberforense

Como se mencionó anteriormente, SureBackup es una característica que no solo prueba la capacidad de restauración del backup, sino que también puede detectar malware. Uno de los objetivos en la fase de respuesta es identificar el tiempo de permanencia del malware, por lo que el uso de marcadores de malware en Veeam Backup & Replication que indican si el malware se ha detectado en un punto de restauración o ha sido encontrado por una herramienta de terceros, facilita la búsqueda para encontrar el primer punto de infección.

Secure Restore es otra función de Veeam Backup & Replication que permite montar discos y analizarlos en busca de malware antes de hacer la restauración completa. Iterar este proceso hasta que se encuentra un punto de restauración no infectado facilita la tarea de encontrar el momento en el que el malware apareció por primera vez en un determinado sistema y le ayuda a evitar la reinfección mediante la restauración de un fragmento de malware inactivo.

Con Veeam Recovery Orchestrator, este proceso de restauración segura puede ejecutarse en todo el entorno con una especie de enfoque orquestado de "sala limpia". Esto no solo agiliza la comprobación de puntos de restauración limpios, sino que añade rápidamente información valiosa para el análisis forense digital de un incidente de ciberseguridad.

Búsqueda mejorada de amenazas con YARA

YARA, una herramienta familiar para los cazadores de amenazas de ciberseguridad, es un enfoque basado en reglas para identificar y clasificar el malware. Una regla de YARA puede identificarse y ejecutarse como parte de una operación de SureBackup o SecureRestore, tanto para la clasificación inicial del malware como para su búsqueda en los backups.

Seguimiento de incidentes con ServiceNow

Gracias a las integraciones directas en ServiceNow, Veeam ONE ahora puede crear automáticamente nuevos casos y actualizar los ya existentes a medida que evoluciona su situación, permitiendo una comunicación más eficiente entre los diferentes equipos y proporcionando una documentación más automatizada del historial del incidente.

Barra lateral: Exfiltración

Si el malware ha accedido a los datos y los ha modificado, entonces es probable que primeramente los haya robado. Los datos exfiltrados son datos que se envían desde el entorno de una víctima a los ciberdelincuentes. Entonces podría convertirse en información publicada o vendida por los ciberdelincuentes después de una infracción, lo que podría suponer secretos corporativos expuestos, reputaciones dañadas e información personal robada que podría dar lugar a futuros fraudes o ciberataques.

Función NIST "recuperar"

Resultado deseado en materia de ciberseguridad:

Desarrollar e implementar las actividades adecuadas para recuperar tras un evento de ciberseguridad (planes, proceso, personas, tecnología)

En función de la naturaleza de su incidente de ciberseguridad, restaurar servicios, especialmente en el caso del ransomware. Si el tiempo de permanencia del malware es largo, muchos puntos de recuperación pueden contener malware, y es posible que deba retroceder mucho en el tiempo para encontrar un punto de restauración limpio. Al igual que con la DR tradicional, es importante alinearse con objetivos que reduzcan al mínimo la pérdida de datos: Sus objetivos de punto de recuperación (RPOs). Dado que descubrir el inicio de su infección es importante en la fase de respuesta, muchos de esos esfuerzos trabajarán en paralelo con el esfuerzo para **recuperar** sus datos.

Un backup solamente es útil si se puede restaurar (y no contiene malware)

El marcado de los puntos de restauración sospechosos o infectados durante las fases de detección y respuesta por características como SureBackup y la API de Incidentes permite identificar fácilmente si se ha detectado malware en cada punto de restauración dentro de la consola de Veeam Backup & Replication. Aunque es un buen punto de partida, no garantiza que sus puntos de restauración anteriores estén completamente limpios.

Para reducir las posibilidades de restaurar datos infectados y el esfuerzo desperdiciado, los esfuerzos de recuperación deben trabajar junto con el análisis ciberforense que se produce en la fase de respuesta. Una sólida asociación de trabajo entre TI, seguridad y el negocio en su conjunto es fundamental para restaurar los datos correctos y no reintroducir el malware.

Si se usan herramientas de detección de malware perfectamente actualizadas como parte de los procesos de SureBackup y Secure Restore, es probable que pueda encontrarse malware que no había sido detectado en un primer momento en puntos de restauración anteriores, por lo que es importante no confiar únicamente en los marcadores de malware de análisis previos. En el caso de que los puntos de restauración limpios se remonten más atrás en el tiempo que sus valores de RPO definidos, pueden usarse restauraciones a nivel de archivo para restaurar fragmentos individuales de datos importantes, evitando así el malware que se esconde en el backup completo.

Restaurar datos no infectados lo más rápido posible

La clave para recuperar rápidamente, incluso en el entorno más simple, es la automatización, pero también es importante fijarse en el modo de restauración. Al utilizar snapshots de cabinas de almacenamiento y recuperación instantánea, los backups restaurados se pueden utilizar casi instantáneamente.

Veeam Recovery Orchestrator se ha diseñado para organizar y establecer todo el proceso de restauración y hacerlo lo más sencillo posible. Al combinar el plan de restauración con los marcadores de infección, Secure Restore, los snapshots de cabinas de almacenamiento, Instant Recovery y la verificación de aplicaciones, Veeam dispone de potente combinación de características para restaurar datos de forma rápida y eficiente, y garantizar al máximo posible que los datos no contengan malware.

Visualización de anomalías I/O

Algunas veces no hay nada que muestre mejor las tendencias que una gráfica visual. Al realizar una recuperación de un trabajo de replicación, la interfaz de usuario de Veeam Backup & Replication muestra gráficas que ayudarán a identificar el momento en el que comenzó el cifrado masivo, lo que reduce el trabajo de encontrar un punto en el tiempo anterior al momento del cifrado.

Barra lateral: Backup vs. replicación para la recuperación de la ciberseguridad

La replicación puede formar parte de su plan de recuperación de ciberseguridad, pero es importante comprender los objetivos de la replicación en comparación con los backups. La replicación se centra en trasladar los datos lo más rápido y volver a la réplica buena más reciente. Los backups no son continuos y, por ello, pueden ser más precisos a la hora de garantizar la limpieza y la capacidad de restauración. La recuperación de un desastre de ciberseguridad debe basarse en el tiempo de permanencia del malware y en la limpieza del punto de restauración, lo que convierte a los backups en un mecanismo más habitual.

Función "Gobernar" del NIST

Resultado deseado en materia de ciberseguridad:

La estrategia, las expectativas y la política de gestión de riesgos de ciberseguridad de la organización se establecen, comunican y supervisan.

La introducción de la función "Gobernar" representa una evolución significativa en la estrategia y supervisión de la ciberseguridad. Esta nueva función hace hincapié en la importancia de la gobernanza en la gestión del riesgo de ciberseguridad de una organización. También subraya la necesidad de establecer políticas, estrategias y procesos de ciberseguridad claros que se alineen con los objetivos generales y la tolerancia al riesgo de su organización. Al integrar la función "Gobernar", NIST CSF 2.0 anima a las organizaciones a adoptar un enfoque más holístico y responsable de la ciberseguridad, lo cual garantiza que las consideraciones de ciberseguridad se inserten en el tejido de la gobernanza organizativa. Esto incluye definir roles y responsabilidades para la ciberseguridad, fomentar una cultura de conciencia de seguridad y garantizar que las decisiones de ciberseguridad estén informadas por los objetivos y restricciones de la organización. La incorporación de esta función pone de manifiesto el cambio hacia el reconocimiento de la ciberseguridad no solo como un desafío técnico, sino como un componente crítico de la gestión empresarial y la resiliencia operativa.

Como componente crítico de la seguridad de los datos, su infraestructura de backup debe cumplir de forma demostrable con las regulaciones gubernamentales y de la empresa. "**Gobernar**" adecuadamente incluye la documentación de la estrategia de gestión de riesgos de ciberseguridad de sus organizaciones, incluidas las configuraciones y políticas, el seguimiento de los cambios y la documentación de los éxitos y fracasos de cada prueba. Esto ayuda a garantizar que las expectativas y las políticas se comuniquen y supervisen de manera efectiva.

Asegúrese de que todo esté documentado

Ya sea para los auditores, los ciberseguros, la mejora de procesos o la seguridad en sí mismo, no se puede sobreestimar a importancia de contar con una documentación precisa, exhaustiva y frecuente. La precisión y la velocidad de un plan de recuperación completamente orquestado ofrecerán el mayor valor posible a los administradores y propietarios de negocios, pero la documentación dinámica creada con cada ejecución completa o de prueba será de gran utilidad para cualquier equipo que necesite evidencia de que realmente funcionó, incluidos los equipos de seguridad y cumplimiento.

Además, el número de informes posibles de Veeam ONE le proporcionará una gran cantidad de información sobre su infraestructura de backup y su estado de salud. Documentar la frecuencia de los backups, el seguimiento de cambios para realizar configuraciones de backup y mucho más son informes integrados que pueden generarse manualmente o de forma programada y luego enviarse automáticamente a los destinatarios adecuados.

Monitorice continuamente para minimizar el riesgo

Aproveche la automatización para verificar las configuraciones de Veeam y el entorno de backup con el fin de asegurarse de que sus dispositivos y software estén seguros y actualizados. Con el Analizador de seguridad y cumplimiento de Veeam, Veeam realiza automáticamente más de 30 comprobaciones de seguridad para garantizar que esté actualizado, que tenga los parches que correspondan y que sus protocolos antiguos e inseguros estén desactivados. Además, toda esta información se compila en un solo informe para que los equipos de seguridad y TI realicen un seguimiento del cumplimiento de las políticas de la organización.

Panel de control de seguridad de backup

La ciberseguridad a menudo consiste en encontrar patrones en su entorno. Dada la amplia variedad de características que Veeam ofrece, incluidas nuevas funcionalidades que se centran en la ciberseguridad, como el panel de control del Centro de amenazas de Veeam, un panel único que agrega múltiples fuentes de datos en la interfaz de Veeam ONE, lo que brinda a los administradores y especialistas en seguridad una vista única de toda su infraestructura de backup.

Conclusión

NIST CSF 2.0 representa un hito importante en la evolución de la gestión de riesgos de ciberseguridad y la lucha contra las amenazas en evolución. Al basarse en la sólida base de CSF 1.1 y al introducir mejoras clave como la función "Gobernar" y un mayor enfoque en la cadena de suministro, CSF 2.0 proporciona a las organizaciones un marco de trabajo más completo y adaptable para ayudarlas a navegar por un panorama de ciberseguridad en constante cambio.

El alcance ampliado de CSF 2.0 garantiza que las organizaciones de todos los tamaños y sectores puedan beneficiarse de su orientación, fomentando así un enfoque más inclusivo y colaborativo de la ciberseguridad. El marco actualizado también reconoce que la gestión eficaz de los riesgos de ciberseguridad requiere la participación activa y el compromiso de las partes interesadas de toda la organización, desde los altos ejecutivos hasta los empleados de primera línea.

En última instancia, el éxito de la implementación de NIST CSF 2.0 se basa en fomentar una cultura de concienciación, colaboración y responsabilidad en materia de ciberseguridad. Al invertir en programas de capacitación y educación, las organizaciones pueden capacitar a su fuerza laboral para que se convierta en participantes activos en el proceso de gestión de riesgos de ciberseguridad. Una comunicación clara y un refuerzo coherente de las políticas y mejores prácticas de ciberseguridad son esenciales para crear un sentido compartido de responsabilidad y vigilancia.

De cara al futuro, es evidente que la ciberseguridad seguirá siendo una prioridad fundamental para las organizaciones de todo el mundo. El aumento de la sofisticación y la frecuencia de las ciberamenazas, junto con la creciente dependencia de las tecnologías digitales, subrayan la necesidad de marcos de ciberseguridad sólidos y ágiles como NIST CSF 2.0. Al adoptar este marco actualizado y comprometerse con su implementación continua, las organizaciones pueden fortalecer su resiliencia, proteger sus activos y mantener la confianza de sus grupos de interés frente a la evolución de los riesgos cibernéticos.

Hoy en día, crear un programa de ciberseguridad no es una tarea fácil. El número de amenazas es muy elevado y el valor de una vulneración para los delincuentes es potencialmente enorme, por lo que las organizaciones deben hacer uso de todas las herramientas a su alcance para crear capas de seguridad de modo que puedan aprovechar al máximo su eficacia en cada etapa del Marco de Ciberseguridad del NIST. Veeam puede aportar valor a todas las etapas del Marco de Ciberseguridad del NIST, mejorando el programa general de ciberseguridad de su organización:

- El hecho de crear y probar regularmente planes de recuperación puede proporcionar datos valiosos que puede utilizar en la fase de identificación para garantizar que los datos críticos estén **identificados** y puedan protegerse.
- Para garantizar que los backups y la infraestructura de backup se tratan de manera adecuada en la fase de **Protección**, es necesario implementar las mejores prácticas y funcionalidades de seguridad nativas documentadas.
- Dado que los backups tocan todos los datos a través de la infraestructura, pueden servir como una segunda comprobación importante para detectar malware que las observaciones del endpoint pueden haber pasado por alto en la fase de **detección** .
- El acceso rápido a diferentes puntos en el tiempo y a entornos virtuales de "sala limpia" puede ser fundamental para los esfuerzos de recopilación de información en la fase de **respuesta** .
- Los backups que se ha determinado que pueden restaurarse y no contienen malware deberán estar disponibles cuando sea necesario y podrán restaurarse a un estado limpio y utilizable lo antes posible para respaldar la fase de **recuperación**.
- Todo el mundo desempeña un papel importante en la seguridad de su organización y sus datos. Establecer, comunicar y hacer una monitorización de la estrategia y las políticas de ciberseguridad de su organización es fundamental en la fase de "**gobernanza**".

Ya ha llegado el momento de que los equipos de TI sean algo más que simples custodios de datos restaurables y pasen a ser participantes activos en el plan de ciberseguridad. Al utilizar las directrices de este documento, los equipos de TI deberían poder mantener una conversación productiva con los equipos de ciberseguridad y las partes interesadas de la empresa para integrar una plataforma de protección de datos basada en Veeam en su programa general de ciberseguridad.

Póngase en contacto con nosotros para obtener más información sobre las funcionalidades y capacidades de Veeam.

Acerca de Veeam Software

Veeam, el líder n.º 1 del mercado mundial en protección de datos y recuperación de ransomware, tiene como objetivo capacitar a todas las organizaciones para que consigan una resiliencia radical a través de la seguridad, la recuperación y la libertad de los datos de su nube híbrida. Con sede en Seattle, oficinas en más de 30 países, Veeam protege a más de 450 000 clientes en todo el mundo que confían en Veeam para mantener sus negocios en funcionamiento. Más información en www.veeam.com o puede seguir a Veeam en LinkedIn @veeam-software y X @veeam.

→ Vea Veeam Data Platform en acción

→ 30 días de prueba gratis