Documento técnico: **2023**

Cómo abordar los principales problemas de seguridad al modernizar la infraestructura del centro de datos

vmware®

Índice

Cómo abordar los principales problemas de seguridad al modernizar la infraestructura del centro de datos

Las empresas modernas tienen la obligación de defenderse ante los impresionantes avances de las amenazas a la ciberseguridad. Para cualquier organización que esté modernizando su infraestructura de nube, esto supone una oportunidad para revisar sus estrategias de seguridad y hacer ajustes que garanticen el cumplimiento de los requisitos de seguridad corporativa.

Los ciberataques amenazan los centros de datos poniendo en peligro la información confidencial que se almacena en sus servidores e interrumpiendo las operaciones esenciales de las empresas. Las empresas suelen almacenar grandes cantidades de datos confidenciales de carácter financiero, personal y empresarial a los que pueden acceder personas no autorizadas con el fin de explotarlos para obtener beneficios económicos o perjudicar a la organización. Existen decenas de categorías de ataques: desde las vulneraciones de datos y el robo de propiedad intelectual, hasta la extorsión y los programas de secuestro. Los programas de secuestro son, indiscutiblemente, los más conocidos. Cuando un atacante consigue impedir el acceso a cosas como los combustibles, los alimentos y los servicios sanitarios a escala nacional, llama la atención de los gobiernos, los clientes y los accionistas por igual.

Además, los centros de datos a menudo sirven de centro neurálgico para la infraestructura de TI de una organización, y un ataque efectivo a un centro de datos puede provocar una interrupción generalizada de las operaciones. Esto puede dar lugar a una pérdida de productividad e ingresos y dañar la reputación de la organización.

Figura 1: La protección de cargas de trabajo es una cuestión de proceso, herramientas y estrategia.

Los ciberataques no son solo una amenaza para la infraestructura de una empresa, sino también para la gestión de sus flujos de caja. Los intentos de mitigar las posibles amenazas pueden repercutir de forma significativa tanto en la inversión en capital como en los gastos operativos, especialmente cuando estas iniciativas no forman parte de una estrategia de seguridad global.

En lo que se refiere a la inversión en capital, es posible que una organización necesite invertir en tecnologías o equipos de seguridad nuevos para mitigar los riesgos de ataques futuros y cumplir los requisitos normativos. Esto puede incluir cortafuegos, sistemas de prevención o detección de intrusiones, y herramientas de cifrado y de seguridad. Estas decisiones pueden generar gastos adicionales imprevistos cuando no se han incluido en un proyecto presupuestado y en un enfoque proactivo continuo.

En cuanto a los gastos operativos, puede que sea necesario aumentar el personal de TI y de seguridad para gestionar y mantener las nuevas tecnologías de seguridad, y formar a otros empleados en la detección de vulneraciones y la respuesta a estas. Si sufre un ataque, la organización también tendrá que dedicar fondos a las investigaciones forenses y la respuesta a incidentes, lo que aumentará sus gastos operativos globales.

La concienciación sobre las ciberamenazas es vital para una estrategia de seguridad eficiente

No todos los ciberataques están diseñados de la misma manera ni tienen la misma finalidad. Los responsables de TI y los arquitectos de seguridad deben ser conscientes de la variedad de ataques, la forma de actuar y los factores de riesgo a la hora de diseñar una estrategia de seguridad eficiente. Es importante señalar que esta no es una lista exhaustiva de todos los tipos de ataques de ciberseguridad, ya que se desarrollan nuevos tipos de ataques constantemente. Por lo tanto, es importante que las organizaciones cuenten con una estrategia de seguridad integral para detectar y responder a tiempo a los incidentes de seguridad.

Los tipos de ciberataques más comunes en el panorama actual

Denegación de servicio distribuido (DDoS)
Estos ataques inundan la red de un centro de datos con una gran cantidad de tráfico, saturándola y evitando que esté disponible para los usuarios legítimos.

Suplantación de identidad
Ataques que utilizan el correo electrónico u otras formas de comunicación para engañar a los usuarios con el fin de que proporcionen al atacante información confidencial, como las credenciales de inicio de sesión.

Programas de secuestro
Ataques que cifran los datos de los servidores de un centro de datos y exigen a la organización un pago a cambio de la clave de descifrado.

Amenazas persistentes avanzadas (APT)
Ataques selectivos diseñados para acceder a la red de un centro de datos y robar información confidencial durante un periodo de tiempo prolongado.

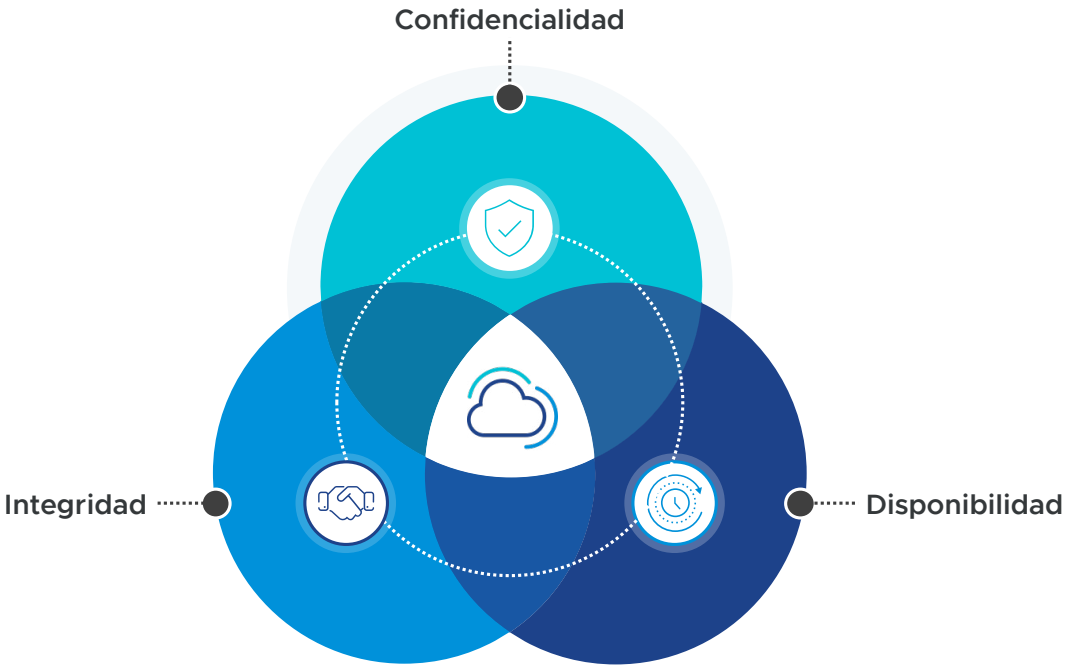
Programa malicioso
Software malicioso que accede a la red de un centro de datos, roba información confidencial o interrumpe las operaciones.

Ataques a la nube
Estos ataques tienen como objetivo las vulnerabilidades de la infraestructura de nube que pueden dar lugar a accesos no autorizados, vulneraciones de datos y otras actividades maliciosas.

Ataques a dispositivos IdC
Estos ataques aprovechan las vulnerabilidades de los dispositivos de Internet de las cosas (IdC), como las cámaras de seguridad y los sensores de temperatura, que están conectados a la red de un centro de datos.

Ataques internos
Estos ataques los lleva a cabo un empleado, un trabajador externo u otro usuario de confianza que tenga acceso a la red del centro de datos.

Qué hay que tener en cuenta al diseñar una arquitectura de seguridad preparada para el futuro



Una buena manera de ilustrar la profundidad de la seguridad necesaria en las plataformas es abordarla desde la óptica de los tres principios básicos de la seguridad de la información: confidencialidad, disponibilidad e integridad.

1. La **confidencialidad de los datos** hace referencia a la protección de la información confidencial para evitar que se acceda a ella o se divulgue a personas o sistemas no autorizados. La confidencialidad de los datos es importante para las organizaciones porque la información confidencial puede utilizarse para obtener beneficios económicos o perjudicar a la organización si personas no autorizadas acceden a ella o la roban.

2. La **integridad de los datos** hace referencia al hecho de que los datos sean exactos y estén completos y a tener la seguridad de que no han sido manipulados, alterados o destruidos de forma no autorizada. La integridad de los datos es importante porque garantiza que los datos que utiliza una organización son precisos, fiables y de confianza. El uso de datos inexactos o manipulados puede provocar decisiones incorrectas, pérdidas financieras y daños a la reputación de la organización.

3. La **disponibilidad de los datos** hace referencia a la capacidad de las personas o los sistemas autorizados para acceder a los datos cuando los necesiten. La disponibilidad de los datos es importante para las organizaciones porque, cuando carecen de acceso a ellos, los procesos empresariales pueden interrumpirse, lo que da lugar a una pérdida de productividad, pérdidas de ingresos y daños a la reputación de la organización. También es esencial para la continuidad de las operaciones, la conformidad con las normativas y la satisfacción del cliente.

Todas las funciones de seguridad de la infraestructura se corresponden con uno o varios de estos principios básicos. Por ejemplo, el cifrado y el enmascaramiento de datos son funciones relacionadas con la confidencialidad de los datos, y la integridad y la aplicación de la función hash a los datos forman parte del principio básico de integridad de los datos.

Todas estas funciones de seguridad están diseñadas para ayudar a las organizaciones a reducir y eliminar riesgos. Este concepto es extremadamente potente, y es la razón por la que las organizaciones preocupadas por la seguridad eligen las plataformas de VMware.

Cómo abordar los principales problemas de la estrategia de seguridad

Al planificar un programa de modernización de la infraestructura de nube, es fundamental que los responsables de infraestructura y operaciones comprendan y aborden los principales requisitos de seguridad para proteger a la organización frente a los ataques y establecer una arquitectura ágil para frustrar los ataques futuros.

Visibilidad y capacidad de observación

La seguridad empieza por la visibilidad. Las empresas no pueden proteger lo que no ven. Sin embargo, la visibilidad no es suficiente por sí sola. La capacidad de observación es la visibilidad inteligente y contextual. Debido a la complejidad de las aplicaciones y las infraestructuras modernas, determinar qué ha sucedido, quién se ha visto afectado y cómo puede solucionarse es más difícil que nunca. Los sistemas de capacidad de observación le permiten inspeccionar y entender la pila de aplicaciones.

La capacidad de observación es un elemento clave en el ámbito de la protección integral. Va más allá de la capacidad de ver, y puede aportar al usuario información contextual sobre lo que ocurre en un sistema dinámico, como los centros de datos definidos por software actuales.

La visibilidad implica comprender qué activos del proceso se están utilizando, por quién, por qué razón y en qué dimensión de interés. Los administradores de sistemas pueden saber mucho sobre la infraestructura observándola en todos sus aspectos desde dentro. Aunque esto pueda parecer un requisito obvio, a menudo se olvida en las políticas y los procesos obsoletos de las distintas empresas. Es importante visualizar y tener información detallada de todos los flujos de la totalidad del centro de datos con una inspección de capa 7 con estado y un contexto completo de las cargas de trabajo, lo que elimina los puntos ciegos de seguridad y acelera la corrección de incidencias.

Implementación de la seguridad basada en políticas

En las infraestructuras definidas por software, la gestión o la arquitectura de seguridad basada en políticas es una manera idónea de definir y controlar dinámicamente la interacción entre los servicios y las aplicaciones. La gestión de la seguridad basada en políticas proporciona funciones de seguridad inteligentes y mejora el control detallado del comportamiento de los usuarios finales.

Sin embargo, las variaciones dinámicas de la red, el rápido aumento de los ataques de seguridad, la distribución geográfica de los nodos y las redes heterogéneas complejas pueden afectar gravemente al rendimiento de las políticas. Cuanto más inteligente sea la definición de la política, más probabilidades tendrá de resistir la evolución de las vulneraciones de seguridad. Por tanto, tan pronto como los responsables de TI comprendan el flujo de las aplicaciones de la infraestructura, los ingenieros podrán definir una forma mejor de proteger las aplicaciones y los activos principales. El uso de un sistema que requiera la menor intervención humana posible hace que el proceso sea más flexible, más escalable y menos propenso a errores.

Garantía de la ejecución de las políticas

Las políticas de seguridad desempeñan un papel importante en el modelo global de seguridad de las empresas. Sin embargo, en muchas organizaciones los desafíos se dividen en tres partes:

1. El desafío de comprender el ámbito de la política (que abordamos con la capacidad de observación)
2. El desafío de definir una política de seguridad completa que lo tenga todo en cuenta
3. El desafío de la implementación inicial y la ejecución

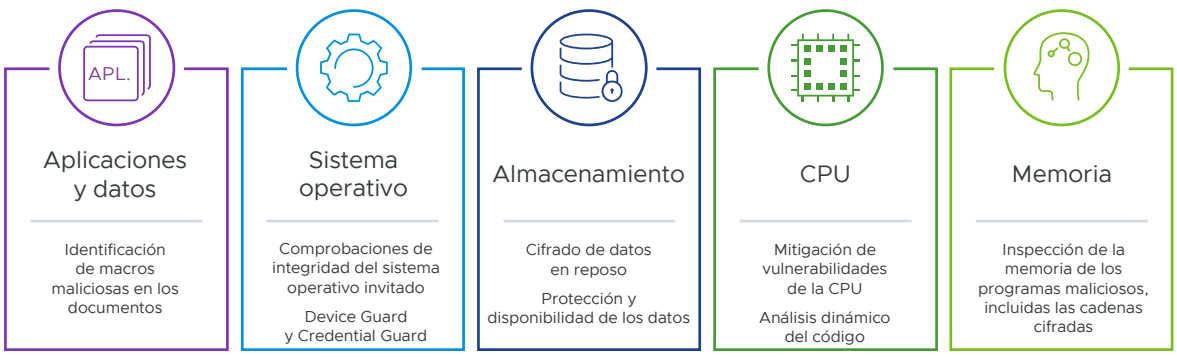
Las organizaciones deben garantizar la existencia de procesos sólidos compatibles con los requisitos de las políticas de seguridad. Los sistemas inteligentes y de automatización, como los proporcionados por VMware NSX® o Advanced Threat Analyzer ayudan a ejecutar estos procesos de forma coherente y más fiable que la intervención humana, que tiene una mayor probabilidad de cometer errores de ejecución.

Implementación de arquitecturas de seguridad modernas con VMware Cloud Foundation

En VMware Cloud Foundation™ (VCF), la seguridad es algo más que enrutadores y conmutadores virtualizados. Los servicios de red y seguridad se distribuyen mediante programación a cada máquina virtual, independientemente del hardware o la topología de red subyacente, de modo que es posible añadir o trasladar cargas de trabajo dinámicamente, y todos los servicios de red y seguridad vinculados a la máquina virtual se mueven con ella a cualquier lugar del centro de datos.

Con NSX, VCF reproduce toda la pila de red mediante software dentro de cada red virtual. Ofrece una arquitectura lógica distribuida para los servicios de capa 2 a 7, lo que incluye elementos lógicos como conmutadores, enrutadores, cortafuegos, balanceadores de carga y VPN.

La seguridad en VMware Cloud: algo más que un cortafuegos



Además de los servicios de red clásicos, los ingenieros pueden utilizar funciones de seguridad completas:

En la capa de aplicaciones:
Es posible identificar macros maliciosas en los documentos.

En la capa del sistema operativo:
Los sistemas operativos se ejecutan en todas partes, por lo que hay que asegurarse de que sean tan seguros como sea posible. Eso significa no solo confiar en el cortafuegos en el ámbito de la máquina, sino también en la infraestructura para protegerse contra los ataques.

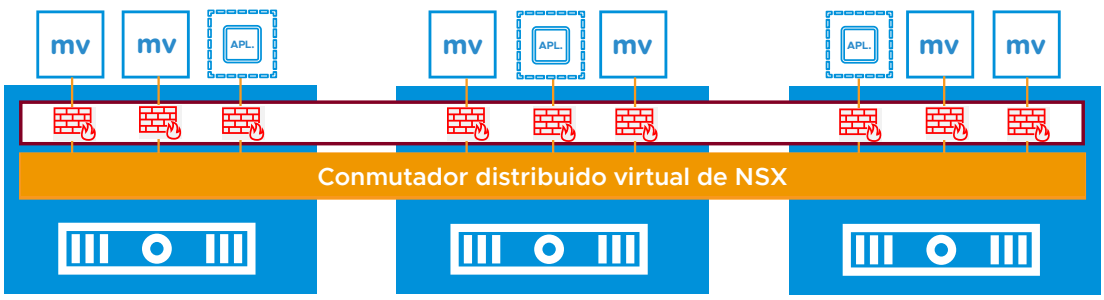
En la capa de almacenamiento:
VMware Cloud Foundation utiliza VMware vSAN™ para almacenar los datos de los clientes y, durante el proceso de almacenamiento, también para protegerlos y cifrarlos, asegurándose de que las políticas de protección de datos mejoradas se actualizan constantemente para hacer frente a las amenazas actuales.

En la capa de hardware:
VMware Cloud Foundation también puede ayudar con los problemas de hardware. No solo hay opciones para el análisis dinámico del código de las cargas de trabajo, sino también para gestionar fácilmente problemas como las vulnerabilidades de la CPU, lo que permite a las organizaciones adaptar su respuesta a sus requisitos empresariales.

Memoria:
VMware NSX Sandbox detecta los procesos y los fragmentos de los programas maliciosos que intentan ocultarse en la memoria y actúa de inmediato para proteger las infraestructuras.

Cortafuegos de nueva generación de VMware Cloud Foundation

Los cortafuegos perimetrales, también conocidos como cortafuegos de red, son una medida de seguridad tradicional que se utiliza para controlar el flujo del tráfico de red entre las redes internas y externas. Aunque los cortafuegos perimetrales pueden proporcionar una valiosa capa de seguridad, también tienen ciertas limitaciones: desde una visibilidad limitada del tráfico interno de la red, pasando por una protección limitada contra las amenazas avanzadas, hasta una protección limitada para los usuarios móviles y remotos.



El cortafuegos distribuido (DFW) es un cortafuegos con estado, lo que significa que supervisa el estado de las conexiones activas y utiliza esta información para determinar los paquetes de red que pueden pasar a través del cortafuegos. El DFW se implementa en el hipervisor y se aplica a las máquinas virtuales a través de su tarjeta virtual de interfaz de red (vNIC). Es decir, las reglas del cortafuegos se aplican en la vNIC de cada máquina virtual. La inspección del tráfico se realiza en la vNIC de una máquina virtual en el momento en que el tráfico está a punto de salir de la máquina virtual y entrar en el conmutador virtual (salida). También tiene lugar en la vNIC cuando el tráfico sale del conmutador y antes de que entre en la máquina virtual (entrada).

Cada máquina virtual tiene su propio contexto y sus reglas de política de cortafuegos. Durante la migración con vMotion, cuando se trasladan máquinas virtuales de un host ESXi a otro, el contexto del DFW (la tabla de reglas y la tabla de seguimiento de conexiones) se traslada junto con la máquina virtual. Además, todas las conexiones activas permanecen intactas durante la migración con vMotion. En otras palabras, la política de seguridad del DFW es independiente de la ubicación de la máquina virtual.

Conclusiones

La seguridad es un aspecto importante de la modernización de los centros de datos que ayuda a proteger los valiosos datos y aplicaciones de una organización frente a los ciberataques. Para proteger los datos confidenciales, es importante implementar medidas de seguridad sólidas, como la segmentación de la red, los cortafuegos, los sistemas de detección y prevención de intrusiones y el cifrado. La modernización de la infraestructura general de los centros de datos permite mejorar la seguridad y adoptar un enfoque más detallado para la prevención de amenazas.

- **El uso de una arquitectura de centro de datos definido por software (SDDC),** como VMware Cloud Foundation permite automatizar y coordinar la infraestructura y la seguridad. Esto facilita la aplicación y el control del cumplimiento de las políticas de seguridad de forma uniforme en todo el centro de datos, así como la respuesta rápida a los incidentes de seguridad.
- **La implementación de la virtualización de red,** por ejemplo, con VMware NSX, que forma parte de VMware Cloud Foundation, permite crear varias redes virtuales dentro de una única red física. Esto permite disponer de un control detallado del tráfico de la red y hace posible la microsegmentación, que ayuda a reducir la superficie de ataque y aislar las distintas cargas de trabajo y aplicaciones entre sí, lo que dificulta el desplazamiento lateral de los atacantes por la red.
- **La implementación del análisis de amenazas mejorado** mediante herramientas como Advanced Threat Protection puede proporcionar a las organizaciones más visibilidad e información sobre las amenazas a la seguridad, así como la capacidad de responder a ellas con mayor rapidez y eficacia.
- **Las funciones de automatización y coordinación** permiten acelerar los procesos de identificación y respuesta a los incidentes de seguridad, utilizando herramientas de seguridad capaces de detectar y responder automáticamente a las amenazas a la seguridad.
- **Mejora de la conformidad:** la modernización de los centros de datos y la optimización de la seguridad pueden ayudar a las organizaciones a cumplir diversos requisitos normativos y de conformidad, tales como HIPAA, PCI-DSS y SOC 2, proporcionando una infraestructura segura y conforme.

La implementación de VMware Cloud Foundation integra todas estas tecnologías y funciones de seguridad modernas en una plataforma de modernización de centros de datos que es segura, conforme a las normativas y ágil.