Parches para el centro de datos

Las empresas apenas pueden dormir con las últimas noticias sobre vulnerabilidades y otras amenazas, además del miedo a lo desconocido o de ser víctima de estas amenazas. Usted está haciendo todo lo que puede para mantener el software del sistema de los usuarios actualizado y seguro. ¿Pero qué ocurre con los servidores en sus centros de datos? En un mundo donde los hackers pueden acceder a códigos ya escritos para aprovechar vulnerabilidades, las empresas necesitan medios efectivos para proteger los servidores de los centros de datos sin agotar los recursos del departamento de TI.

Sus prácticas de seguridad deben incluir la gestión de parches para mantener los servidores reforzados, los datos seguros y disponibles y la reputación de su empresa intacta. Debe desplegar los últimos parches de seguridad a la vez que dedica tiempo a los objetivos principales de la empresa.

Usted necesita controles e informes precisos sobre el proceso de parcheo completo: descubrimiento e inventario de parches y despliegue de todos los parches disponibles en su entorno continuamente y con un horario adecuado para su organización.

Sin embargo, muchas organizaciones tienen problemas para mantener el software de los servidores con las últimas actualizaciones de software para sistemas operativos y aplicaciones de terceros, como los sistemas Microsoft Windows® y el hipervisor VMware vSphere®. El problema es que los centros de datos presentan más problemas de gestión de parches que los sistemas de los clientes.

Detección y resolución del centro de datos completo

Para proporcionar una gran precisión en los parches de su entorno, debe poder encontrar fácilmente los parches que faltan mediante análisis de sistemas y desplegar parches según políticas en todo su entorno. Sin una visibilidad clara de su entorno e información detallada para saber qué sistemas son los más vulnerables, es imposible entender los riesgos de su empresa. Sin embargo, esto no es fácil debido a las diversas configuraciones disponibles en los centros de datos modernos.

Las limitaciones de tiempo y presupuesto asociadas con un entorno de centro de datos virtual (la espera a que se carguen, parcheen y apaguen máquinas virtuales (VM)) hace que algunas personas ignoren los entornos virtuales y asuman riesgos innecesarios. Centrarse solamente en los servidores físicos deja la empresa expuesta y existe peligro de no pasar una auditoría. Debe poder encontrar vulnerabilidades, escanear parches no aplicados y desplegarlos en servidores físicos y virtuales fácilmente sin alterar la carga de los servidores o la empresa. En cuanto al cumplimiento, no se pueden ignorar los sistemas offline. Debe garantizar el cumplimiento de los parches y entregar actualizaciones de software tanto si el sistema está en la red o desconectado.

Reduzca el tiempo de parcheo

Teniendo todo esto en cuenta, ¿cuánto tardan actualmente sus procesos de actualización del software en sus centros de datos? ¿Meses o semanas? Para reducir el riesgo, debe reducirlo a días y horas.

Tradicionalmente, un 50 % de los ataques ocurren de dos a cuatro semanas tras el lanzamiento. Un SLA de parches obligatorio a los 14 días le proporcionará una ventaja contra la mayoría de ataques. Pero los procesos manuales, prácticas y herramientas múltiples que no soportan todo su entorno aumentan la complejidad de la gestión, igual que el tiempo que se tarda en descubrir, definir y entregar paquetes de actualizaciones y en aplicar estos parches críticos.

Independientemente de si sus sistemas están conectados o desconectados, debe ahorrar tiempo y dirigir sus preciados recursos a acciones con un resultado inmediato y de gran valor.

Hay muchas formas de reducir el tiempo y el riesgo. Por ejemplo, las plantillas de parches ahorran tiempo y reducen el riesgo cada vez que crea un servidor. La capacidad de encontrar rápidamente sus máquinas virtuales offline y de parchear estas máquinas virtuales y plantillas puede ahorrarle hasta una hora por sistema. Mantener las imágenes offline constantemente listas para su despliegue le garantiza que puede desplegar una máquina virtual sin tener que preocuparse de si está actualizada.

La forma más eficaz de ahorrar tiempo es automatizar el proceso completo de parcheo de servidores. Considere su reacción actual a las evaluaciones de vulnerabilidad de fabricantes. Encontrar todos los parches relacionados con las vulnerabilidades comunes (CVE) y crear grupos de parches automáticamente puede ahorrarle mucho tiempo.

Finalmente, debe simplificar el cumplimiento con informes al recortar la enorme cantidad de información en su entorno y acceder a los datos que necesita. Proporcionar los datos adecuados a los ejecutivos, directores y propietarios de aplicaciones proporciona fácilmente la visibilidad necesaria para pasar auditorías y una información actualizada sobre su postura de seguridad para una mejor toma de decisiones.

Lista de verificación de la gestión de parches

Automatizar su proceso de gestión de parches (desde el descubrimiento a la evaluación y el despliegue) en todas sus estaciones de trabajo y servidores físicos y virtuales, online y offline, le ayudará a reducir el tiempo de entrega de parches de seguridad críticos. La lista a continuación puede ayudarle a encontrar la solución de parcheo adecuada.

Ivanti puede ayudarle

Gracias a un robusto y sencillo parcheo de servidores que cumple todos sus requisitos, Ivanti puede ayudarle a proteger su centro de datos para que pueda ahorrar tiempo y dinero y centrarse en apoyar las iniciativas clave de la empresa. Las herramientas de Ivanti pueden estar listas en cuestión de minutos para ayudarle a descubrir, evaluar y resolver sus sistemas en el centro de datos automáticamente en función de las políticas definidas. Nuestras herramientas simplifican el parcheo en sus sistemas físicos y virtuales. Encuentre estaciones de trabajo y servidores online y offline, busque parches que no se han instalado y despliéguelos. Entonces parchéelo todo desde el SO y las aplicaciones a máquinas virtuales (VM) e incluso el hipervisor ESXi con nuestra gran integración con VMware.

Característica	Descripción
Administración	Punto de administración único basado en función
Descubrimiento, inventario y parcheo automatizados	Proteja estaciones de trabajo de clientes, servidores físicos, servidores virtuales, hipervisores y plantillas
Actualizaciones del SO	Sistemas operativos Windows y Linux
Parcheo de aplicaciones	Aplicaciones de terceros y personalizadas
Listas de parches automatizadas a partir de CVE	Importe listas de evaluación de vulnerabilidades de cualquier fabricante
Contenido de parches	Acceda a un gran catálogo de parches
Despliegue de parches	Despliegues con agente, sin agente o basados en la nube
Reversión de captura	Capacidad de hacer copias de seguridad antes de aplicar parches
Habilitador de automatización	APIs para automatización y orquestación
Colaboración	Comparta el estado y verifique el cumplimiento de parches con otros
Informes	Paneles de control en tiempo real e informes personalizados

Leer Más
www.ivanti.es +39 347 6335127 contact@ivanti.es