¿Puede un Antivirus Proteger Completamente Su Centro De Datos?

¿Puede un Antivirus Proteger Completamente Su Centro De Datos? A pesar de la creencia popular, los centros de datos no son «a prueba de balas» contra los ataques de piratas informáticos. Puede tener más peligro si posee un servidor porque los ciberdelincuentes se enfrentarán a usted con toda su fuerza.Pero,¿Un antivirus serviría?Es lo que vamos a mostrar en este artículo de nuestro blog.

Hay bastantes productos antivirus en el mercado, pero no todos son adecuados para un centro de datos. La buena noticia es que, con un antivirus de alta calificación, puede dejar de preocuparse por las amenazas externas.

Para decirlo, un centro de datos es un hardware que contiene información (para empresas, gobiernos, etc.). Además, el hecho de que se pueda acceder a estos datos desde cualquier rincón del mundo convierte los centros de datos en una herramienta útil. Todas las partes autorizadas pueden obtener la misma información sin tener que visitar la ubicación del centro de datos. Sin embargo, dado que la información se transfiere libremente entre varias computadoras, eso hace que sea más fácil para los delincuentes obtenerla .

Protección para un centro de datos.

Se puede vender información valiosa a partes rivales o usarla para chantajear a los dueños de negocios. El cifrado, la protección con contraseña, la seguridad del protocolo y los firewalls son muy eficaces . Aún así, ningún centro de datos estará a salvo sin un antivirus adecuado. Los archivos corruptos de la empresa pueden desaparecer para siempre, y el

malware avanzado es capaz de destruir grandes cantidades de datos (a menos que haya un antivirus para eliminarlo).

Cuando se trata de centros de datos, hay tres «puntos» principales que necesitan protección. Estos incluyen el escritorio, el servidor y la puerta de enlace. Repasemos cada uno y veamos cómo una solución antivirus puede ayudarlo a proteger la información crítica. Cada uno de los puntos que acabamos de mencionar tiene sus pros y sus contras: también hablaremos de ellos.

Protegiendo el escritorio

En el pasado, la protección del escritorio era la única «área» donde se usaban los antivirus. En estos días, sigue siendo crucial para asegurar los centros de datos , pero tiene una gran desventaja. La cuestión es que, para que funcione, cada usuario final necesita actualizar su software regularmente. Además, es difícil hacer un seguimiento de todos ellos, lo que pone al centro en peligro.

Los antivirus de escritorio modernos tienen numerosas notificaciones automáticas. Es común que las personas se olviden de ellos, los pospongan o los ignoren, lo que, nuevamente, hace que todo el sistema sea vulnerable. Así es como funciona la protección de escritorio: el antivirus escanea las unidades y la RAM (memoria), buscando código malicioso de la base de datos.

Además, en el segundo que encuentra un archivo / aplicación potencialmente peligroso, el usuario recibe una notificación. A continuación, el usuario puede elegir una de las siguientes acciones: eliminar el virus, tratar de limpiar los archivos / aplicaciones o ponerlos en cuarentena. Eso es todo lo que necesita saber sobre la protección antivirus de escritorio. No es perfecto, pero, hasta el día de hoy, los centros de datos lo incluyen como una sólida capa de defensa.

Protegiendo el servidor

En este caso, la solución antivirus funciona en el nivel del servidor de correo electrónico. Eso significa que la mayoría de los códigos maliciosos serán eliminados incluso antes de que lleguen a las computadoras de los usuarios. Lamentablemente, incluso con un antivirus que protege los servidores, los virus logran ingresar a la red. La protección del servidor es tan importante como la protección del escritorio, pero, en la mayoría de los casos, viene como un «bono», y es por eso que las compañías internacionales lo usan.

Si solo confía en el antivirus del servidor y el malware ingresa a los escritorios, nada evitará que corrompa / destruya datos comerciales confidenciales. Por lo tanto, debe usarlo todo junto, incluida la protección siguiente (y final), en el nivel de «puerta de enlace». Funciona de manera similar a la protección del servidor, pero tiene un enfoque ligeramente diferente.

Protegiendo el Gateway

La idea aquí es detener el malware en el punto más alejado, mucho antes de que tenga la oportunidad de llegar a la red. Mientras los virus / mensajes corruptos se mantengan a raya, no podrán dañar el centro de datos. Las puertas de enlace no han existido durante mucho tiempo, pero ya han demostrado ser una valiosa adición a la protección a nivel de servidor y escritorio.

La integración del software antivirus en el hardware de la red es el corazón y el alma del enfoque de puerta de enlace. A nivel de puerta de enlace, el antivirus escanea todos los mensajes entrantes, buscando posibles amenazas. Además, cuando encuentra mensajes infectados, los detiene, los pone en cuarentena o los elimina. Según los expertos, esta solución con visión de futuro es muy prometedora y, muy probablemente, se convertirá en la nueva normalidad en los próximos años.

Con productos integrados integrados directamente en las redes, será mucho más cómodo proteger los centros de datos de amenazas externas. Debe saber que los gobiernos mundiales también utilizan el enfoque de centro de datos / servidor, y esa es una de las razones por las cuales la seguridad de los puntos finales se está convirtiendo en una gran parte del mundo en el que vivimos ahora.

El servidor de Windows es el sistema operativo de servidor más popular y fácil de usar, y hasta el día de hoy, las empresas están utilizando Win Server 2003, a pesar de que 2016 ya está disponible. En muchos sentidos, 2003 es la versión del servidor de Win XP, mientras que 2012 es el equivalente del servidor de Win 10. Antes de comprometerse con cualquier software antivirus, no olvide compararlo con otros productos y asegúrese de que sea exactamente lo que necesita .

Tener un virus por su cuenta, dispositivo personal es una cosa; poner en peligro un servidor completo debido a un

antivirus defectuoso es una historia completamente diferente. Escaneo automático, modo silencioso y bajo impacto en el sistema: esas son algunas de las cualidades que debe buscar en un antivirus de servidor.

Ver otros recursos útiles del blog al respecto: Cómo diseñar un data center o centro de datos eficiente y rentable; ¿Por qué necesita copias de seguridad externas? ; ¿Ransomware puede afectar a servidores web Linux ?