En esta ocasión os presentamos un interesante artículo de nuestro amigo Raül MONTALA, Preventa de Bitdefender, y especialista en Seguridad, donde nos comenta la importáncia de la seguridad en los entornos virtuales y la criticidad de los mismos.

La información y los servicios que gestiona un datacenter son críticos. El nivel de seguridad que requiere no es el mismo que el de los puestos de trabajo de la organización. Una solución diseñada específicamente para entornos virtualizados garantiza mayor seguridad, integración y estabilidad para el datacenter. Además, añade una doble protección antivirus, conviviendo con las protecciones existentes. ¿Garantiza un antivirus tradicional la seguridad del datacenter? Por varias razones, en Bitdefender creemos que no.

Durante los últimos años, la virtualización y el cloud computing han ido subiendo escalones hasta convertirse en el estándar a seguir para que una empresa trabaje de manera ágil y eficiente con las tecnologías de la información.

En la última década, la virtualización dejó de estar presente sólo en grandes empresas para aparecer en las PYMEs donde son los proveedores de servicio los que le sacan ventaja.

Inicialmente se virtualizaron los entornos de desarrollo, fue entonces cuando algunos servicios críticos también se sumaron. En ese momento y sin darnos cuenta, la virtualización entró de manera silenciosa hacia los entornos de producción de las empresas. Hoy en día existen empresas que cuentan con toda su infraestructura virtualizada.

‘’ La realidad es que el antivirus tradicional instalado en entornos virtualizados afecta a la seguridad y al rendimiento. ‘’

Servidores, equipos, almacenamiento, aplicaciones y hasta comunicaciones son algunos ejemplos que pueden virtualizarse. Todo esto sin importar dónde estén alojados los servicios, ya sea en las propias empresas o en datacenters externos.

Así como los entornos físicos (no virtualizados) necesitan servicios esenciales como el antivirus, copia de seguridad, correo electrónico, software de gestión, etc. Los entornos virtualizados necesitan exactamente lo mismo, con la diferencia que los servicios se han adaptado al entorno; pasando a ser híbridos.

Refiriéndonos al antivirus, lo habitual es aprovechar la misma protección que está instalada en el entorno físico e instalarla en el entorno virtualizado. Los proveedores de antivirus tradicionales han reaccionado tarde ante la virtualización, es por eso que este tipo de soluciones no están a la altura para proteger el datacenter.

‘’ Las empresas tienden a proteger el datacenter con la solución antivirus que está instalada en los equipos físicos.”

Bitdefender estuvo presente tanto en el VMworld como en el Citrix Synergy, eventos oficiales de los dos fabricantes líderes en virtualización; celebrados a finales del pasado año en Barcelona. Después de varias entrevistas con visitantes, quedó confirmado que el antivirus tradicional instalado en entornos virtualizados afecta a la seguridad y al rendimiento, y es una preocupación cada vez mayor.

Inicialmente puede parecer cómodo o práctico, pero son varias las razones por las que, en Bitdefender, creemos que es un error. Los antivirus tradicionales fueron diseñados para trabajar en equipos físicos conectados a una red local. El núcleo de un antivirus tradicional tiene servicios como los motores de análisis, o las actualizaciones, servicios que se instalan en cada equipo. Cuando un antivirus tradicional se instala en una máquina virtual, lo interpreta como si esta fuera una máquina física; generando una serie de problemas que afectan a la seguridad, estabilidad y sobre todo al rendimiento del datacenter.

Este tipo de soluciones carecen de integración con la tecnología de virtualización, de modo que exigen un trabajo manual sobre todo en la instalación y la administración. La duplicidad en el análisis o la gestión de las actualizaciones son otros desafíos generados por los antivirus tradicionales. Cuando se detecta una infección en red, independientemente de donde proceda; también es detectada por otras máquinas virtuales, generando duplicidad y consumo de recursos locales. Es decir, a parte del problema que la infección como tal genera, se le añade el de rendimiento. Por otro lado, los análisis bajo demanda consumen elevados recursos de

procesador y memoria, pudiendo dejar las máquinas virtuales saturadas y en consecuencia el datacenter.

La gestión de las actualizaciones es un problema que puede desencadenar otros. Las actualizaciones residen en cada máquina virtual. Por lo tanto, si en un entorno virtualizado tenemos máquinas virtuales apagadas, congeladas o con instantáneas; cuando arranquen tendrán que actualizarse. Este lapso de actualizaciones deja a las máquinas virtuales susceptibles a recibir ataques de día cero y además las máquinas virtuales generan tráfico mientras se actualizan.

La realidad es que **el nivel de seguridad que requiere un datacenter no es el mismo que tienen los equipos físicos. La información y los servicios que gestiona un datacenter son sumamente importantes, sensibles y críticos para la empresa.**
Destacando también la capacidad que el datacenter debe tener en cuanto a alta disponibilidad y replicación, los servicios y aplicaciones deben estar a la altura y no pueden permitirse fallos o caídas. La presencia de Malware en los puestos de trabajo de la organización genera mucho trabajo de sistemas y un problema de pérdida de productividad; pero lo realmente dramático es si este Malware entra en el datacenter y accede a los sistemas productivos que soportan la actividad y el negocio. Las consecuencias pueden ser desastrosas y en definitiva se pierde tiempo y dinero.

Entonces, ¿Por qué confiar la seguridad del datacenter a soluciones antivirus que no han sido diseñadas para entornos virtualizados?

Existen soluciones antivirus en el mercado compatibles con cualquier tecnología de virtualización y que han sido diseñadas específicamente para securizar estos entornos. De hecho, dos soluciones antivirus distintas, una para el datacenter y otra para los equipos físicos, pueden convivir y se recomienda separar los dos niveles de seguridad. Frente a una infección habrá dos motores de detección; garantizando mayor fiabilidad y otro punto de vista.

Security for Virtualized Environments (SVE) es la solución de Bitdefender diseñada específicamente para entornos virtualizados. Las principales ventajas de SVE son el análisis centralizado, junto con las actualizaciones y la administración, compatibilidad con cualquier tecnología de virtualización, importante ahorro de recursos y el mejor motor de detección.

El análisis centralizado lo realiza un appliance virtual de seguridad hacia todas las máquinas virtuales del datacenter, liberando el antivirus local de cada máquina virtual y protegiéndola de inmediato cuando arranca. El mismo appliance gestiona las actualizaciones pudiendo tener las máquinas virtuales al día aunque estén apagadas, congeladas o con instantáneas.

‘’ SVE centraliza el análisis liberando el antivirus de las máquinas virtuales, y generando un importante ahorro de recursos ‘"

Desde una consola de administración central, tenemos visibilidad del estado de la seguridad de todo el datacenter. Si hay una infección, avisa claramente de dónde procede pudiendo tomar acciones de manera inmediata.

Sólo con el hecho de centralizar el análisis y las actualizaciones, se genera un importante ahorro de recursos. Si comparamos la media de consumo de un antivirus tradicional, con SVE se pueden multiplicar los recursos disponibles 2.5x. De media se ahorra un 30% en procesador y un 10% en memoria. El impacto frente al rendimiento de aplicaciones es sólo del 9%. Se estima que una empresa con 1000 escritorios virtualizados se ahorra aproximadamente $500K en tres años, de modo que el retorno de inversión aumenta.

Entidades independientes como AV-Test o AV-Comparatives han galardonado a Bitdefender como mejor antivirus del pasado 2012. Las pruebas hacen referencia a detección, destacando el mayor número de Malware detectado y el menor de falsos positivos. Estas comparativas demuestran que cuota de mercado y los mejores motores de detección no parecen precisamente sinónimos. Los fabricantes más extendidos en las grandes instalaciones parecen más interesados en hablar de costes y continuidad que en invertir en poner al día sus motores.

Desde Bitdefender creemos que el datacenter necesita una solución diseñada para trabajar en ese entorno y que no es incompatible con la solución antivirus instalada en los equipos físicos. Garantizamos una excelente detección, integración y ahorro de recursos. SVE es una solución fácil de implementar, administrar y altamente escalable.

Seguridad silenciosa para entornos que darán mucho de qué hablar.

Raül Montalà, Sales Engineer para España, Bitdefender.

Si deséas mayor información puedes solicitarla pulsando aquí.