

Cuatro factores a tener en cuenta si intenta ahorrar en seguridad

Autor: Mark Bouchard

AimPoint Group
keeping IT on target

Resumen ejecutivo

La incesante presión para hacer más con menos ha obligado a los directivos de todo el mundo a perseguir ávidamente técnicas y tecnologías que ahorren costes tales como la consolidación de los centros de datos, la virtualización de los servidores y el uso de software como servicio (SaaS). Y, quizás, esta presión es aún mayor en el ámbito de la seguridad de la TI. Los niveles de riesgo siguen disparándose al mismo tiempo que los recursos disponibles para contener las amenazas asociadas, en el mejor de los casos, se han congelado.

Una vez más, la consolidación es una respuesta razonable. Implementar sistemas de seguridad multifuncionales, tales como gateways de seguridad para la red, gateways de seguridad para el correo electrónico o incluso dispositivos de gestión unificada de las amenazas (UTM), así como centrarse en suites de soluciones en vez de en productos puntuales, son técnicas que suelen dar excelentes resultados. No obstante, cuando evalúen estas soluciones, los administradores de TI/seguridad deben evitar caer en la trampa de conceder demasiada importancia a los costes iniciales de adquisición, licencias y mantenimiento. El verdadero coste de cualquier solución y, por lo tanto, su potencial para ofrecer ahorro con respecto a las alternativas disponibles, también depende de cuatro factores adicionales: la eficacia de la seguridad, la eficiencia administrativa y operacional, la amplitud de la cobertura y la adaptabilidad, cada uno de los cuales puede variar considerablemente de una solución a otra.

El panorama de la seguridad de la información

El reto al que se enfrentan las organizaciones actuales es realmente desafiante. Alcanzar una mayor eficiencia operacional sin dejar de ser competitivos nos obliga a adoptar abiertamente la tecnología de la información. El despliegue constante de nuevas aplicaciones y tecnologías de comunicación y el aumento de su exposición a componentes externos son, básicamente, un imperativo empresarial. Las organizaciones, sin embargo, deben ofrecer de forma simultánea un nivel efectivo de confidencialidad, integridad y disponibilidad para la infraestructura, las aplicaciones y, lo más importante, la información relacionadas. Asimismo, deben seguir por esta senda incluso cuando aumentan los niveles de riesgo y se congelan los recursos financieros y de otro tipo.

Los niveles de riesgo siguen en aumento

Solo es necesario tener en cuenta los tres elementos que integran la ecuación clásica del riesgo (amenazas, vulnerabilidades y valor de los recursos) para comprender lo que está pasando.

- **Las amenazas.** La presencia de una economía sumergida para la información de valor ha provocado una explosión en la cantidad de amenazas creadas, así como en la velocidad con la que se desarrollan y distribuyen.
- **Las vulnerabilidades.** La superficie abierta a los ataques sigue creciendo a medida que la presión de la competencia obliga a las organizaciones a adoptar paulatinamente tecnologías emergentes, comprar y crear nuevas aplicaciones y aceptar mayores grados de movilidad de los usuarios, interconectividad y acceso de terceros a los sistemas conectados en red.
- **El valor.** El valor de los recursos de la información está aumentando en paralelo a la creciente dependencia de las organizaciones modernas por la información electrónica y los sistemas asociados. La red, por ejemplo, se ha convertido en un elemento profundamente arraigado en el modo de realizar negocios.

Los recursos siguen limitados

A pesar de todo esto, los presupuestos en seguridad para TI no están aumentando de forma proporcional. Lo que es más, en algunos casos están disminuyendo. Esto es debido en gran medida a la debilitada economía y a los retos que presenta para la mayoría de las empresas de todo el mundo. Otras fuerzas que también entran en juego son la autocomplacencia y una creciente sensación de inutilidad.

En el primer caso, relativamente pocos ataques importantes han ocupado los titulares en los últimos años, por lo que algunos equipos de gestión han llegado a la conclusión de que en estos momentos no es realmente necesario realizar más inversiones en la seguridad de la información.

Al mismo tiempo, los niveles de frustración están disparándose puesto que siguen produciéndose con frecuencia incidentes e infracciones significativas, a pesar de las sumas cada vez mayores destinadas a la seguridad de la información durante años. Como resultado, algunos equipos de gestión están básicamente dispuestos a capitular, al menos hasta el punto de que, ahora, tener una garantía sustancialmente mayor de la eficacia de una solución es un requisito previo antes de realizar ninguna otra inversión.

La tiranía de la realidad

Aunque las causas específicas son verdaderamente debatibles, la base del problema no lo es: cuando se trata de la seguridad de la TI, la inmensa mayoría de las organizaciones quieren poder hacer más con menos. Naturalmente, muchas de esas organizaciones están buscando modos de reducir costes.

Con esta situación, no es sorprendente que los productos de seguridad de bajo coste ostenten cierto grado de atractivo. Sin embargo, el problema radica en que, con demasiada frecuencia, las soluciones que parecen especialmente prometedoras a primera vista muestran una plétora de costes ocultos que se hacen dolorosamente obvios después de empezar a funcionar. Los elementos de coste fijos (aquellos asociados al hardware, las licencias y el mantenimiento) representan solo un aspecto del coste total de propiedad de una solución, por lo que es muy imprudente darles demasiada importancia. De hecho, a las organizaciones que no tienen en cuenta este factor de riesgo a la hora de reducir costes les puede salir el tiro por la culata.

Sin pretensión de sonar alarmista, este es un mensaje que merece ser repetido, especialmente durante periodos de dificultades económicas, cuando la competencia entre los proveedores es más despiadada que nunca.

El modo adecuado de reducir los costes en seguridad

Además del punto iniciado en el apartado anterior, el modo correcto de conseguir un ahorro de costes duradero e incluso más sustancial a la hora de elegir soluciones de seguridad de la información es mirar más allá de los costes fijos y obvios. Hay cuatro factores que los administradores de TI/seguridad deben tener particularmente en cuenta para reducir costes de forma recurrente: la eficacia, la eficiencia, la amplitud de cobertura y la adaptabilidad de una solución.

La eficacia es la tarea n.º 1

El primer y más importante de todos los factores que determinan el verdadero coste de una solución es su eficacia, es decir, su capacidad de bloqueo. Los productos que no pueden evitar permanentemente la introducción o ejecución de amenazas, tanto conocidas como no conocidas, pueden acabar representando un coste importante para una organización. Cada suceso de infección conlleva, como mínimo, el coste considerable de "limpieza" o el esfuerzo necesario para restaurar los sistemas a una configuración adecuada y, con suerte, más sólida¹. Los incidentes de mayor calibre también ocasionan costes sustanciales como notificaciones a los clientes, la pérdida de datos, multas por incumplimiento de normativas, indemnizaciones por daños y perjuicios, deterioro de la confianza de los clientes y/o pérdida de la ventaja competitiva.

En otras palabras, la "ineficacia" en este caso se mide de forma relativa. Ningún producto de seguridad será nunca eficaz al 100%. Por otro lado, una solución que esté un 5-10% por detrás de las mejores, no ahorrará dinero a una organización a largo plazo, independientemente de lo inferior que sea su coste inicial.

Los elementos de coste fijos (aquellos asociados al hardware, las licencias y el mantenimiento) representan solo un aspecto del coste total de propiedad de una solución, por lo que es muy imprudente darles demasiada importancia.

¹ Cada año, en una empresa con 5.000 empleados, casi dos tercios de los puntos finales sufren una infección causante de un coste en mano de obra de TI de más de 197.000 \$ por limpieza/restauración de cada punto final – *The Cloud-Client Enterprise Security Impact Report*, Osterman Research, enero de 2009.

Y aunque la eficacia relativa es complicada de determinar definitivamente, en gran medida porque varía con el tiempo, es sencillamente demasiado importante como para ignorarla. De este modo, a continuación se exponen algunos indicadores, imperfectos aunque útiles, que las organizaciones pueden usar para evaluar la eficacia de una solución:

- **¿Cuál es su historial?** Más allá de una herencia y pasado sólidos, también debemos encontrar pruebas de un éxito continuado y actual de la solución. Idóneamente, esto debe adoptar la forma de pruebas piloto comparativas realizadas en condiciones reales. Sin embargo, dado el coste asociado, es posible que nos tengamos que conformar con resultados de pruebas publicados en fuentes independientes.
- **¿Usa técnicas innovadoras?** ¿Qué técnicas o "ingrediente especial" incluye la solución para contrarrestar las características imperantes del panorama de las amenazas, más rápidas, diversas y esquivas? A modo de ejemplo, contar con el respaldo de una extensa red de información sobre amenazas y poder usar una arquitectura de Internet-cliente (que reduce la dependencia de actualizaciones locales para tener al día la protección) permite a una solución "detectar más amenazas y antes"². Junto con estas capacidades, el empleo de un control de acceso adaptado a cada aplicación, las firmas de prevención de intrusiones orientadas a las vulnerabilidades y los algoritmos de detección heurísticos posibilitan una mayor capacidad de bloqueo sin necesidad de tener detalles específicos sobre las amenazas.
- **¿Cuál es el grado de integración de sus componentes?** Parece obvio que compartir la información entre las tácticas defensivas individuales que conforman una solución aumente su eficacia. Un ejemplo sencillo es cuando la detección de malware en el material descargado de un sitio Web activa una función complementaria de filtrado de URL que evita automáticamente que otros usuarios accedan a la página o al dominio responsable³.

Las múltiples facetas de la eficiencia

El segundo factor más importante para determinar la capacidad real de una solución para reducir costes es su eficiencia. Algunos aspectos de la eficiencia son bastantes obvios: la facilidad de gestión y la capacidad de automatización, por ejemplo, mientras que otros son algo menos evidentes. Los siguientes elementos que se sugiere evaluar incluyen ambos aspectos.

- **¿En qué punto se frustran las amenazas?** De forma genérica, las amenazas como el malware se pueden frustrar en diversas etapas: mediante el bloqueo del acceso a los recursos que las contienen en primer lugar; detectando y eliminándolas en el momento de la descarga; o bien neutralizándolas una vez que han alcanzado un punto final y se empiezan a ejecutar. Contar con distintas funcionalidades a lo largo de estas etapas es absolutamente necesario. Sin embargo, aquellas que se centran en las primeras etapas, tales como el filtrado de URL dinámico/reforzado por la evaluación de la reputación y el bloqueo del spam, podríamos decir que son las más importantes. Esto se basa en el hecho de que minimizan la carga de trabajo de la infraestructura final, incluido el ancho de banda de la red, los gateways de seguridad y los sistemas de puntos finales.
- **¿Cuál es el impacto de la solución en su entorno?** Estrechamente relacionado con el elemento anterior, este se refiere a la presencia de técnicas innovadoras que ayuden a reducir los requisitos administrativos y de recursos. Por ejemplo, para soluciones antimalware y para puntos finales, una arquitectura de Internet-cliente ofrece una clara ventaja: elimina la necesidad de realizar actualizaciones convencionales de firmas con frecuencia cada vez mayor para garantizar el máximo grado de protección, una tarea que, de lo contrario, requiere un esfuerzo considerable por parte del personal de TI, consume un ancho de banda importante y capacidades de los dispositivos de la red y

² Una arquitectura de Internet-cliente es aquella donde una cantidad sustancial de la información sobre las amenazas está alojada en la red. Las soluciones de seguridad que usan esta arquitectura no tienen que retener un serie de recursos basados en los contenidos (p. ej., firmas o URL) en cada componente local, sino que, en vez de ello, complementan una lista parcial y entradas en caché al realizar llamadas en tiempo real a un extenso almacén centralizado que se actualiza de forma constante.

³ Aunque los ejemplos incluidos anteriormente se centran predominantemente en la seguridad antimalware, de contenidos y puntos finales, los principios generales, la argumentación y los consejos son aplicables también a la mayoría (si no a todos) del resto de los dominios de la seguridad de la información.

merma significativamente la productividad de los usuarios finales. Añadir la reputación de archivos y la capacidad de detección relacionada amplía aún más estas ganancias porque ayuda a controlar el tamaño de los archivos de firmas que se deben mantener en los sistemas locales y mejora la eficiencia de las interacciones entre Internet y los clientes.

- **¿Es la solución sencilla de usar y mantener?** Las características de configuración y supervisión centralizadas y unificadas son clave para una verdadera solución escalable, como también lo es la capacidad para distribuir e implementar automáticamente actualizaciones de contenido y firmware. Menos común, pero bastante potente desde una perspectiva de reducción de costes, es la capacidad de reparar una infección de malware automáticamente.

El arte de cubrir múltiples bases de una sola vez

Técnicamente, este tercer factor también se podría clasificar como otra "faceta de la eficiencia". Sin embargo, tratarlo por separado ayuda a enfatizar su significado. La idea general es que, siempre que no introduzcan elementos que comprometan los factores anteriores, las soluciones que ofrecen una amplia cobertura pueden ayudar a reducir el coste total de la seguridad. De hecho, el uso estratégico de gateways de seguridad multifunción y suites de software bien estructuradas evita la necesidad de usar varias herramientas de gestión, mantener e integrar toda una colección de productos para puntos dispares y negociar y mantener una gran cantidad de relaciones con los proveedores. Hay incluso algunas conexiones que ayudan a reforzar aún más la eficacia de la eficiencia. Por ejemplo, la visibilidad centralizada de múltiples controles puede acelerar la detección de las amenazas, la confirmación y la respuesta, mientras que una función unificada de creación de informes simplifica la de otro modo onerosa tarea de compilar pruebas para auditorías de cumplimiento de normativas.

En términos del alcance real de la cobertura que ofrece una solución concreta, hay tres dimensiones que los administradores de TI/seguridad deberían evaluar:

- **Cobertura de funcionamiento.** Para hacer frente a la creciente diversidad de amenazas se requieren varias tácticas defensivas que incluyan una mezcla de técnicas de detección de modelo positivo, modelo negativo y específicas del tipo (p. ej., rootkit), junto con funciones de prevención y supervisión.
- **Cobertura lógica.** En última instancia, la protección necesita llegar a todas las capas de la infraestructura informática, desde la red hasta las aplicaciones, e incluso hasta los mismos datos.
- **Cobertura física.** De forma similar, no es suficiente proteger solo el perímetro. La cobertura idónea debería extenderse de extremo-a-extremo, lo que significa tener tácticas defensivas en los puntos conflictivos externos e internos, así como cerca o en los propios puntos finales individuales.

Flexibilidad y adaptabilidad = Seguridad a bajo coste en el futuro

Las soluciones de seguridad que son muy adaptables y, por lo tanto, pueden seguir siendo aplicables a pesar del cambio de condiciones, pueden reducir definitivamente la necesidad de inversiones adicionales en el futuro. Por el contrario, las soluciones que estén inevitablemente vinculadas a un elemento de hardware, sean difíciles de actualizar o no puedan adaptarse a la creciente demanda del funcionamiento por pasos y la modificación de los modos de funcionamiento (p. ej., computación en nube), serán las responsables en última instancia de aumentar los costes debido a su vida útil, significativamente más corta.

Las opciones de configuración flexibles, una admisión amplia de plataformas, la integración sin problemas con soluciones de otros fabricantes y la capacidad de admitir totalmente otras iniciativas de reducción de costes que pueda aplicar la organización son consideraciones todas ellas válidas en este aspecto.

Otro elemento que actualmente tiene cada vez más importancia es la compatibilidad con la virtualización. Disponer de una versión de appliance virtual para las tácticas defensivas basadas en red implica varias ventajas. Además de soler tener un gasto inicial menor, la necesidad de solo desarrollar software, frente a un sistema entero, y el hecho de que la implementación solo implica software y/o una clave de licencia significa que los nuevos controles para contrarrestar las nuevas amenazas se pueden aplicar e implementar más rápidamente que con los appliances convencionales.

Los appliances virtuales, sin embargo, son solo el principio. La virtualización es una tendencia mucho más amplia con muchas facetas adicionales, la mayoría de las cuales se persiguen debido a su potencial para conseguir ahorros sustanciales de los costes. Por lo tanto, lo que los administradores de TI/seguridad preocupados por los costes necesitan evaluar es cómo encajarán las soluciones de seguridad candidatas desde una perspectiva más amplia, ofreciendo múltiples opciones, no solo para proteger la infraestructura virtualizada sino también para poder formar parte de ella.

Conclusión

El aumento de los niveles de riesgo y la reducción de los presupuestos han puesto a las organizaciones actuales en una situación difícil: no pueden permitirse dejar de implementar la tecnología de la información ni de realizar las inversiones correspondientes, pero hacerlo de modo relativamente seguro es cada vez más complicado. Encontrar formas de reducir costes y usarlos como un modo de estirar los recursos disponibles es verdaderamente una respuesta acertada. Lo que no es acertado, sin embargo, es ignorar los elementos del coste total de propiedad que van más allá de los costes por licencias y mantenimiento. En concreto, los administradores de TI/seguridad necesitan centrarse en la eficacia, la eficiencia, la amplitud de la cobertura y la adaptabilidad, ya que son estos cuatro factores los que determinan el verdadero coste de una solución y su potencial último para ayudar a las organizaciones a hacer más con menos.

Acerca del autor

Mark Bouchard, CISSP, es el fundador de AimPoint Group, una empresa de investigación y análisis de TI especializada en seguridad de la información, gestión del cumplimiento de normativas, entrega de aplicaciones y estrategias de optimización de infraestructuras. Antiguo analista de META Group, Bouchard ha valorado y pronosticado las tendencias empresariales y tecnológicas para una amplia gama de temas de seguridad de la información y redes durante más de 13 años. Durante este tiempo, ha asistido a cientos de organizaciones en todo el mundo con iniciativas estratégicas y tácticas por igual, desde el desarrollo de estrategias de varios años y arquitecturas de alto nivel a la justificación, selección e implementación de soluciones de seguridad y redes. Veterano de la Marina de los EE.UU., Mark Bouchard presta una ayuda entusiasta a las empresas para que puedan afrontar mejor sus retos de TI.

Los administradores de TI/seguridad necesitan centrarse en la eficacia, la eficiencia, la amplitud de la cobertura y la adaptabilidad, ya que son estos cuatro factores los que determinan el verdadero coste de una solución y su potencial último para ayudar a las organizaciones a hacer más con menos.