Seguridad Proactiva – El blindaje empresarial contra las amenazas tecnológicas

LIBRO BLANCO

Objetivo del documento

Defenderse de la multitud de riesgos de seguridad en la actualidad puede suponer una gran inversión de recursos, especialmente para aquellas empresas en expansión que necesitan protegerse contra las mismas amenazas que azotan a grandes corporaciones, pero contando sólo con una pequeña parte de los recursos informáticos que utilizan éstas.

La finalidad de este documento es examinar el panorama de riesgos actuales y explicar cómo la implementación de una solución de seguridad integrada puede ofrecer a las empresas una mayor protección que un conjunto de soluciones básicas, además de un importante ahorro en los costes.

La evolución del *malware*

Proteger la red de una empresa nunca ha supuesto un desafío tan grande como hoy en día. La industria del *malware* se ha profesionalizado y los creadores de código malicioso han dejado de ser esos jóvenes "traviesos" que realizaban simples intentos al azar de *ciberbandalismo*. Actualmente los intentos de los criminales organizados están orientados a la sustracción económica, información personal o confidencial, o una suma de ambas. Esta motivación lucrativa ha servido para incrementar tanto la sofisticación como la frecuencia de los ataques dando como resultado un *malware* cada vez más difícil de detectar, mucho más que los virus creados por los s*cript kiddie* del pasado. Además de tener en cuenta formas cada vez más complejas de ataques, las empresas deben lidiar con el *spam* y con nuevos riesgos, como el uso inadecuado de Internet por empleados o el incumplimiento de los mismos respecto a las políticas corporativas de seguridad.

El crecimiento de las necesidades en tecnología de la información (TI) es directamente proporcional al crecimiento de los riesgos que nos rodean. El mundo empresarial, armado con sus últimas creaciones en tecnología móvil, equipos portátiles totalmente equipados y la demanda de un acceso 24 horas al día, 7 días a la semana, hace necesario abrir nuevos e innumerables puntos de acceso a la red de una compañía – puntos de acceso que sobrepasan muchas de las soluciones perimetrales tradicionales-. Además, los dispositivos móviles que no estén protegidos, o que lo estén de forma incorrecta, pueden infectar una red empresarial poniendo en peligro la integridad de los datos y el funcionamiento normal de la empresa. Por esta razón, la seguridad en las terminales se ha convertido en algo tan vital como la seguridad perimetral, aunque asegurarse de que los dispositivos móviles o terminales frecuentemente desconectadas son seguros, puede acarrear muchas dificultades.

El panorama actual de riesgos

Hoy en día, las empresas necesitan protegerse contra una serie de amenazas cada vez más diversas, rápidas y sofisticadas que provienen tanto del interior como del exterior.

- **La red de redes.** La web se ha convertido en el medio de transmisión de ataques elegido y lidera la lista del Instituto SANS "Top Ten Cyber Menaces for 2008"[1]. Las vulnerabilidades presentes en muchos navegadores y sus *plug-ins* han ofrecido a los atacantes blancos fáciles. Los ataques a través de páginas web también han crecido en cuanto a su complejidad, intentando explotar múltiples vulnerabilidades a la vez que utilizan mecanismos cada vez más sofisticados con el objetivo de mantener oculta su carga dañina a los productos de seguridad. Además, no son sólo las páginas web las culpables de los riesgos que corren por la red; los sitios web legítimos son habitualmente atacados y configurados para expandir código malicioso. Esto es especialmente problemático a la hora de que los usuarios apliquen diferentes configuraciones de seguridad en sitios web que a simple vista parecen confiables o que tengan menos cuidado cuando navegan por las mismas.

- **Proliferación de Malware.** El malware se ha incrementado a niveles epidémicos con más de 5 millones de virus nuevos o variantes identificados durante 2007[2], lo que supone 4 millones más que los que fueron descubiertos en 2006. Adicionalmente, los virus destructivos han sido desbancados como la principal amenaza por otro tipo de malware no destructivo con una variación en sus objetivos focalizándose hacia el robo de datos y dinero.

- **Crecimiento del *phishing*.** Los ataques de *phishing* se están convirtiendo en algo habitual. Según los datos de la consultoría Gartner, 3,6 millones de personas perdieron más de 1.900 M€ a través de estafas de phishing durante los 12 meses anteriores a agosto del 2007[3]. Los consumidores no son el único objetivo de ataques de phishing, las empresas también están siendo atacadas cada vez con mayor frecuencia. En ataques a objetivos específicos ("*spear phishing*") la información pública disponible es utilizada para crear mensajes que parecen tener una alta credibilidad, pero que por el contrario, llevan cargas maliciosas. En 2006, la red del departamento de estado de los EEUU fue puesta en peligro con código malicioso adjunto que contenía un correo de "*spear phishing*". Mientras que los ataques en grandes corporaciones y departamentos gubernamentales atraen todas las miradas, las empresas en expansión tienen el mismo riesgo ya que son percibidas como un objetivo fácil por los criminales.

- **Pérdida de productividad y recursos de la red.** El *spam* se ha convertido en una pandemia global que en 2007[5] costó a las empresas alrededor de 65.000 M€. En el pasado, el *spam* se usaba como una herramienta de mercadeo utilizada por "granujas de poca monta"; actualmente, es utilizado por organizaciones criminales para perpetrar estafas *pump-and-dump*[6] con las que limpian millones de euros.

- **La descomposición de perímetro de la red.** Los ordenadores portátiles y dispositivos móviles electrónicos se han convertido en un quebradero de cabeza para los departamentos informáticos. Esta dificultad fue uno de los temas estrella entre los participantes que acudieron a la conferencia InfoSecurity Europe[7] en 2007. Reforzar la política de seguridad en dispositivos móviles puede resultar difícil y, por ello, algunos dispositivos no pueden estar totalmente seguros, ya que éstos pueden utilizarse como vía para propagar malware dentro de las redes empresariales de forma que puedan eludir las soluciones perimetrales de seguridad tradicionales.

- **Conviviendo con la amenaza.** El abuso de Internet por parte de los empleados se ha convertido en uno de los mayores problemas para muchas empresas. En el Reino Unido se estima que la pérdida de productividad debida al uso de portales de redes sociales como Facebook durante la jornada laboral, cuesta a las empresas más de 8.000 M€[8] y el 20% del ancho de banda de la red. Si a eso se añade el tiempo malgastado en páginas como eBay o simplemente navegando sin objetivo laboral, los costes de tiempo y dinero siguen incrementándose. Para terminar de agravar el problema está el hecho de los sitios de redes sociales poseen usos comerciales útiles, y por tanto una total prohibición de su uso no sería la solución..

Mientras la frecuencia de los ataques se incrementa y sofistica, también hay que tener en cuenta el hecho de su interconexión. La información recogida en las páginas web de redes sociales es utilizada para realizar campañas de *phishing*. El código malicioso difundido por las campañas de *phishing* a través de emails se apropia de los ordenadores para sus redes "zombie"[9] (redes de ordenadores controlados y utilizados remotamente para propósitos criminales sin el conocimiento ni consentimiento de los propietarios de los mismos). Los *botnets* o redes *zombie* se utilizan para propagar *spam* que contiene código malicioso o enlaces que apuntan a páginas web infectadas, que a su vez infectan a otros equipos que participarán en las campañas de *spam* masivas, ataques DoS o de denegación de servicio, enviar *phishing* a través de email o distribuir más *malware* todavía.

El problema real con el que se encuentran las empresas hoy en día no es tanto como defenderse contra los distintos tipos de amenazas (en la actualidad ya existen productos que dan protección a cada necesidad de protección) sino cómo defenderse de ellos mediante una alta calidad de protección a un coste óptimo.

El problema con las soluciones básicas

Las soluciones de seguridad estándar que cubren parcialmente los aspectos importantes, como los detectores de intrusión o sistemas de prevención (IDSs y IPSs), soluciones antivirus, filtros web o *spam* e innumerables productos similares que efectúan funciones esenciales, sólo cubren las necesidades de aquellas infraestructuras de seguridad que poseen un elevado nivel de soporte. Cada aplicación estándar nos llevará a otra aplicación que deberá unirse a la primera y que, por tanto, debe instalarse, configurarse, actualizarse y mantenerse, así como gestionar otro proceso de venta. Cada solución adicional aumenta la complejidad de la infraestructura y requiere una mayor inversión en mano de obra tecnológica y formación para utilizar correctamente la nueva herramienta. Además, hay que añadir a la complejidad de la estructura el incremento del riesgo de los errores humanos, lo que introducirá agujeros de seguridad no intencionados.

A corto plazo, aunque las soluciones estándar parecen ser efectivas, traen consigo un alto incremente en el Coste Total de Propiedad (TCO)

BitDefender Business: Incrementando la seguridad y disminuyendo el Coste Total de Propiedad (TCO)

Las soluciones de seguridad para empresas de BitDefender, han sido diseñadas desde el principio hasta el final para ofrecer inmejorable nivel de protección con un bajo Coste Total de Propiedad (TCO)

- **Bajo TCO pasando por la optimización de productividad.** Los costes de adquisición de una solución de seguridad están muy por debajo de su TCO (Costes de soporte y gestión continua) Las productos para empresas de BitDefender han sido diseñados para hacer tan fácil su gestión y su racionalización como inferior el coste TCO.

  - ✓ **Políticas de seguridad.** BitDefender Management Server incluye una serie de políticas de seguridad que pueden implementarse de forma fácil y rápida usando plantillas genéricas personalizables. Estas políticas pueden utilizarse para controlar cualquier aspecto del comportamiento del producto BitDefender, incluyendo la configuración de la programación de actualizaciones, del antimalware, configuración del cortafuego y del *antispam*, así como sus respuestas específicas a cualquier evento tanto de seguridad como de cualquier tipo. Las políticas "offline" de BitDefender permiten a los administradores tener la certeza de que los equipos continúan cumpliendo con las políticas de seguridad incluso cuando se desconectan de la red y no pueden comunicarse con el servidor de gestión. BitDefender también puede configurarse automáticamente para reforzar las políticas de seguridad en cada equipo conectado a la red instalando el módulo de cliente en ellos y bloquearlo hasta que alcance un nivel de seguridad determinado.

  - ✓ **Integración con Active Directory (AD).** Los grupos creados en AD pueden replicarse en el servidor de gestión de BitDefender y personalizar las políticas aplicadas en cada grupo, adaptándose a la arquitectura de red existente en la empresa.

  - ✓ **Administración centralizada.** La gestión centralizada de la consola de BitDefender ahorra tiempo a los administradores debido a la posibilidad de administrar cada módulo desde un mismo lugar.

La eficiente gestión de BitDefender permite ofrecer un muy bajo coste de TCO a través de la mejora de productividad del administrador.

- **Protección integrada segura.** BitDefender elimina el coste y complejidad asociados al mantenimiento de diferentes soluciones estándares, integrando la protección contra virus, troyanos, *rootkits*, *spyware*, *spam*, *phishing* y ataques "*zero day*" y otras amenazas dentro de una única y fácil solución de gestión.

  Adicionalmente, BitDefender permite a las empresas protegerse contra el abuso que los empleados hacen de Internet, configurando reglas para limitar o bloquear el acceso a aplicaciones o a páginas web que presenten algún riesgo de productividad o seguridad (Ej. Aplicaciones de mensajería instantánea y páginas web de redes sociales). BitDefender es altamente configurable y permite a la empresa no sólo elegir entre bloquear aplicaciones o sitios web, sino restringir su uso a ciertas horas o ciertos grupos de trabajo.

- **Escalabilidad.** Mientras algunas soluciones se vuelven poco prácticas cuando se gestiona un alto número de ordenadores debido a los retrasos en la comunicación entre servidor y cliente, la comunicación unidireccional basada en HTTP utilizada por BitDefender requiere solamente unos mínimos recursos de la red. BitDefender puede, además, continuar satisfaciendo las necesidades de las empresas en crecimiento y permitir a través de las habilidades existentes su expansión.

- **Seguridad de primer nivel.** BitDefender ofrece una de las protecciones más robustas y fiables de la industria. Los productos BitDefender han sido certificados por los laboratorios independientes ICSA y Checkmark y han obtenido numerosos reconocimientos VB100. Además, BitDefender es uno de los fabricantes de la industria de la seguridad que ofrece uno de los más rápidos tiempos de respuesta frente a las nuevas amenazas.

Sumario

Para protegerse contra el panorama, cambiante y de rápida evolución actual de constantes riesgos, muchas empresas se están encontrando con que sus infraestructuras de seguridad son cada vez más caras y difíciles de gestionar.

Las soluciones de seguridad para empresas de BitDefender ayudan a las organizaciones a simplificar sus estructuras de seguridad fusionando la protección contra virus, *malware*, *spam*, *phishing* y cortafuego en una única solución de gestión centralizada. Reforzando la gestión de esta manera, las soluciones empresariales de BitDefender permiten ahorrar a las organizaciones tanto tiempo como dinero. Además, permitiendo reforzar su política de seguridad de los dispositivos móviles, ayuda a las empresas a protegerse ante uno de los mayores restos de la seguridad actual: la seguridad en los puntos finales.

Y lo que es más importante, una organización que utiliza las soluciones para empresas de BitDefender puede estar tranquila sabiendo que su red está totalmente protegida por una de las soluciones de seguridad líderes del mercado.

Sobre BitDefender:

BitDefender es el fabricante de una de las líneas más efectivas y rápidas de software de seguridad, certificado a nivel internacional. Desde sus comienzos en el 2001, no ha parado de mejorar y crear nuevos estándares en cuanto a protección proactiva se refiere. La gama de productos de BitDefender protege diariamente a 10 millones de hogares y empresas en todo el mundo, dándoles la tranquilidad de saber que sus gestiones digitales se realizarán de forma segura. Las soluciones BitDefender se distribuyen a través de una red global de distribuidores con valor añadido en más de 100 países de todo el mundo. Para más información, visite: www.bitdefender.es

Bibliografía

[1]Top Ten Cyber Security Menaces for 2008
http://www.sans.org/2008menaces/?utm_source=web-sans&utm_medium=text-ad&utm_content=text-link_2008menaces_homepage&utm_campaign=Top_10__Cyber_Security_Menaces_-_2008&ref=22218

[2]Quantity of malware booms
http://www.heise-security.co.uk/news/101764/from/atom10

[3]Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks
http://www.gartner.com/it/page.jsp?id=565125

[4]House Committee on Homeland Security Subcommittee on Emerging Threats, Cyber Security, and Science and Technology (statement of Donald R. Reid, Bureau of Diplomatic Security)
http://homeland.house.gov/SiteDocuments/20070419153111-10569.pdf

[5]Industry Statistics (Ferris Research)
http://www.ferris.com/research-library/industry-statistics/

[6]Microcap stock fraud
http://en.wikipedia.org/wiki/Microcap_stock_fraud

[7]Security's Top Five Priorities
http://www.darkreading.com/document.asp?doc_id=123294

[8]UK takes £6.5bn hit from Facebook & company
http://www.telegraph.co.uk/money/main.jhtml?xml=/money/2008/01/22/bcnface122.xml

[9]Botnet
http://en.wikipedia.org/wiki/Botnet

[10]Denial-of-service attack
http://en.wikipedia.org/wiki/Denial-of-service_attack