Gli antivirus non sono tutti uguali

White Paper Sophos

Giugno 2005

RIEPILOGO

Poiché i maggiori produttori di soluzioni antivirus offrono delle soluzioni i cui tassi di rilevazione sono pressoché uniformi, si tende a credere che i prodotti antivirus siano “tutti uguali”. Tuttavia, una valutazione approfondita del Total Cost of Ownership (costo totale di proprietà) dei prodotti antivirus deve prendere in considerazione sei fattori principali. In realtà, esistono enormi differenze tra i produttori che interessano le prestazioni, la rilevazione delle minacce informatiche, il focus, le piattaforme supportate, il supporto tecnico e la facilità di gestione.

Prestazioni

Uno degli aspetti chiave della protezione antivirus sono le prestazioni. Le prestazioni del motore antivirus a livello del desktop e del server si ripercuotono direttamente sulla produttività degli utenti. Tanto più veloce è il prodotto antivirus ad eseguire la scansione, e tanto più efficiente è l’aggiornamento del motore antivirus con le definizioni dei virus più recenti, quanto minore sarà l’impatto sulla produttività degli utenti finali: quando si tratta di scansione antivirus la rapidità è un fattore decisivo. Una delle conseguenze derivanti dall’utilizzo di un software dalle prestazioni scarse è l’impatto negativo sulla sicurezza. Il personale IT resta spesso sorpreso nello scoprire che le applicazioni antivirus sono tra quelle che utilizzano la maggiore quantità di risorse di sistema. Purtroppo, molti responsabili IT, le cui aziende utilizzano le soluzioni antivirus di altri produttori, sono spesso sconcertati dal fatto che gli utenti finali differiscono o annullano la scansione antivirus sui desktop. Alcuni prodotti, infatti, utilizzano una quantità eccessiva di risorse e impiegano troppo tempo per eseguire la scansione o l’aggiornamento, compromettendo la stabilità del desktop. Ciò determina una falla pericolosa nella sicurezza e complica il compito del personale IT di garantire la conformità dell’intera azienda alle politiche di

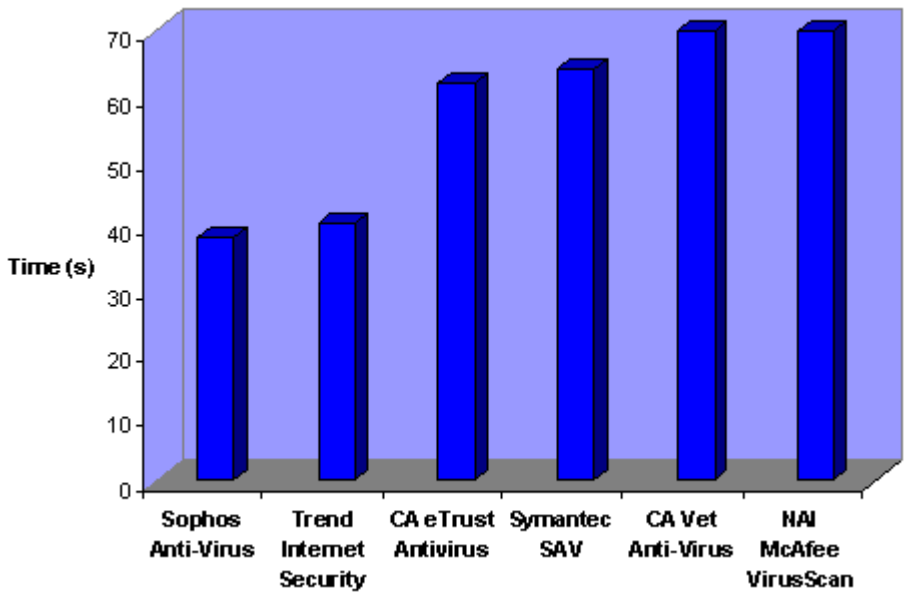

Figura 1. Velocità media di scansione dell'hard disk – software antivirus a confronto (Fonte: Analisi comparativa condotta da Virus Bulletin nel 2004).

sicurezza. Test indipendenti hanno confermato ripetutamente che le prestazioni di Sophos Anti-Virus™ sono superiori a quelle di tutti gli altri principali prodotti antivirus (vedere figura 1). Il motore antivirus di Sophos offre velocità elevate di scansione, risultando di facile utilizzo per l'utente. La differenza consiste nel fatto che gli altri prodotti antivirus sono altrettanto efficienti nella rilevazione dei virus, ma in alcuni casi difficili da distribuire e da eseguire correttamente sull'intera rete aziendale. Queste difficoltà si traducono nell'impossibilità dell'azienda di restare conforme alle normative vigenti nei vari Paesi. L'obiettivo di queste leggi è la protezione delle informazioni. I dati originali non devono essere alterati in alcun caso e ad ogni tentativo di modificare o distruggere le informazioni deve far seguito un allarme. I virus, lo spyware e i software malevoli possono compromettere persino i dati gestiti nel modo più accurato. Alcune norme richiedono che le aziende impediscano persino ai worm nuovi e sconosciuti, contenuti nei messaggi e-mail, di infiltrarsi nella rete aziendale. Altre tutelano i dati dal punto di vista amministrativo, tecnico e fisico.

Threat detection

La connettività ha accresciuto la vulnerabilità delle imprese, che è aggravata dalla natura in continua evoluzione delle minacce informatiche. La rapidità con la quale le nuove minacce informatiche vengono create e si propagano via Internet rende i computer degli utenti finali più vulnerabili che mai. Per rilevare le minacce informatiche, viene utilizzato un modello suddiviso in quattro componenti principali, come illustrato nella figura 2 qui sotto.

I mezzi sui quali si può contare per la rilevazione delle minacce informatiche rappresentano un aspetto fondamentale. Sophos adotta un approccio complesso alla gestione della sicurezza dei propri clienti. In primo luogo, il **Threat Detection Network** ha l'obiettivo di raccogliere tempestivamente informazioni sulle ultime minacce informatiche presenti su Internet. Una combinazione di trappole per lo spam, i cosiddetti honeypot, sparse sulla Rete raccolgono continuamente informazioni in tempo reale, fungendo da sistemi di preallarme in caso di attacco. In secondo luogo, lo spam e i virus raccolti vengono quindi analizzati dai SophosLabs™, una rete globale di centri di ricerca e analisi che vigila 24 ore su 24, 7 giorni su 7 sui nuovi software malevoli e sulle nuove campagne di spam. Ciò consente a Sophos di reagire rapidamente e di gestire in modo più efficiente gli attacchi combinati di spam e virus.

I SophosLabs effettuano una serie di analisi automatizzate per scoprire gli schemi e le caratteristiche comuni a diverse minacce informatiche. In terzo luogo, Sophos aggiorna tempestivamente le definizioni dei virus, garantendo una protezione proattiva costante. Infine, la protezione viene implementata sulla rete del cliente nei principali punti strategici - gateway, server e desktop - assicurando la miglior difesa disponibile. La principale responsabilità dei SophosLabs è di distribuire gli aggiornamenti dei file di identità dei virus ai clienti Sophos. Il fattore decisivo di quest'operazione sono i tempi di reazione. Senza una protezione aggiornata, un'azienda rischia di essere vulnerabile all'attacco delle

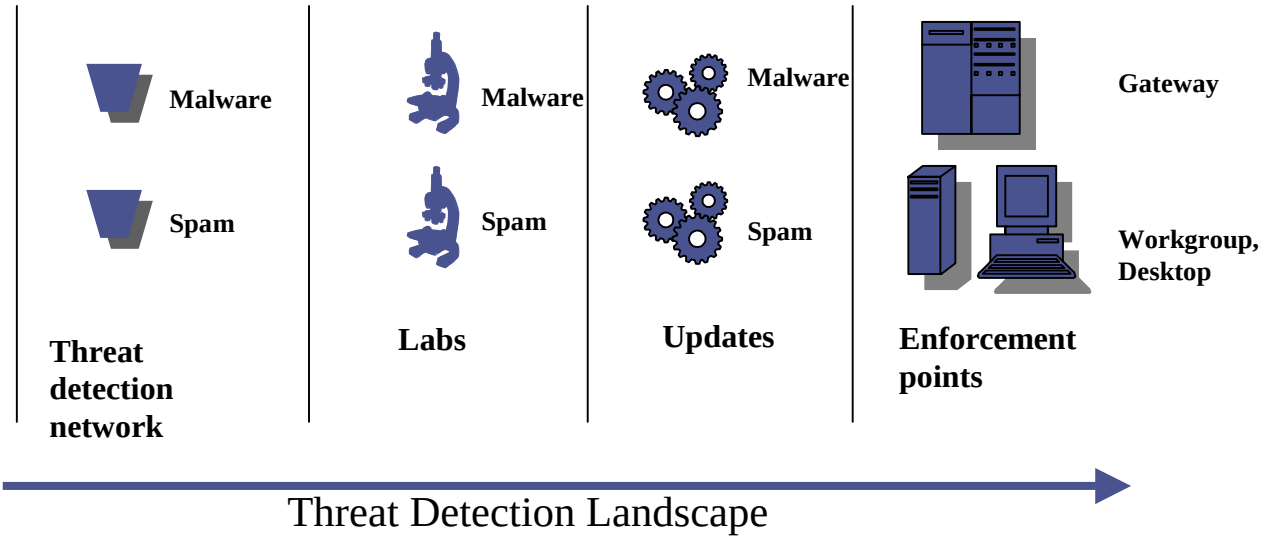

Figura 2: Le quattro componenti della rilevazione delle minacce informatiche.

minacce informatiche più recenti. La reattività del produttore è cruciale, poiché la rapidità degli attacchi dei virus è notevolmente aumentata. Per esempio, il virus SQL Slammer ha infettato 250 mila server in 10 minuti.

Come illustrato nella figura 3, i tempi di reazione di Sophos, presentati in forma di tabella nell'ambito di un test effettuato da terzi nel 2004, sono stati più brevi rispetto ad altri principali produttori di soluzioni antivirus: le dimensioni degli aggiornamenti delle definizioni dei virus variano notevolmente tra i produttori principali. Le dimensioni degli aggiornamenti incrementali di Sophos si aggirano intorno ai 5KB. La distribuzione di un aggiornamento di questa entità su una rete di grandi dimensioni (per esempio, 20.000 desktop) impiega di solito 30 minuti o meno. Un altro aspetto importante della rilevazione delle minacce informatiche, sul quale i produttori di soluzioni antivirus concentrano la propria attenzione, è la proattività. La tecnologia Genotype™ di rilevazione dei virus di Sophos è in grado di rilevare in modo proattivo le varianti conosciute dei virus. Analizzando la struttura dei primi esempi di un virus, gli esperti di Sophos creano un sistema che identifica le famiglie di virus. Nel caso dei virus Mydoom e Bagle, in cui molteplici varianti dello stesso virus furono messe in circolazione in un breve lasso di tempo, la tecnologia Genotype è stata in grado di rilevare e di gestire il virus in tempo reale, senza protezione aggiuntiva. Quindi, i clienti Sophos sono costantemente protetti dai virus, anche da quelli nuovi e sconosciuti per i quali non esiste ancora la protezione specifica.

Produttore	Tempi medi di reazione
Sophos	Meno di 8 ore
Trend Micro	Meno di 10 ore
CA	Meno di 12 ore
McAfee	Meno di 14 ore
Symantec	Meno di 16 ore

Figura 3: Confronto dei tempi di reazione dei produttori su un periodo di 9 mesi nel 2004 (Fonte: Anti-virus Outbreak Response and Impact – AV-Test GmbH).

Target: mercato B2B

Nella scelta di una soluzione antivirus per la propria azienda, è importante optare per un prodotto che risponda alle esigenze di gestione della rete aziendale. Queste esigenze sono molto differenti e molto più complesse di quelle di un utente domestico. I produttori principali offrono sia soluzioni per l'utenza aziendale, sia soluzioni per il mercato consumer. Per esempio, una grossa fetta degli utili di Symantec nel segmento antivirus proviene da quest'ultimo settore.

L'architettura dei prodotti Sophos è stata studiata per la protezione "top down" della rete, diversamente dagli altri produttori che hanno tentato di adattare un prodotto antivirus lato client alle esigenze di protezione delle grandi reti. I prodotti Sophos sono venduti soltanto alla clientela business e tutta l'attività di sviluppo mira a fornire le funzionalità e i miglioramenti adatti a questo mercato.

Piattaforme supportate

Molte aziende hanno operato investimenti consistenti nei sistemi come Windows 95/98, OpenVMS e NetWare, nonché in varie piattaforme Linux e UNIX, e questi investimenti continuano a offrire benefici. Con l'esigenza crescente di ridurre il budget del reparto IT e di contenere i costi, queste aziende sono estremamente riluttanti a smantellare i propri sistemi, a spese e a rischio dei processi aziendali. Un produttore di soluzioni antivirus come Sophos offre una protezione uniforme su un'ampia gamma di piattaforme e tutela l'investimento già operato dalle aziende. Grazie al supporto per numerose piattaforme, infatti, Sophos consente alle aziende di far fruttare i propri investimenti nell'hardware, senza dover effettuare un upgrade del sistema. L'upgrade viene spesso richiesto dagli utenti finali che desiderano prestazioni migliori, sebbene, con tutta probabilità, il loro desktop o notebook attuale sia sufficiente ad eseguire MS Office e altre applicazioni aziendali. Sophos supporta la gamma di piattaforme (desktop e server) più ampia fra tutti i principali fornitori di soluzioni antivirus:

- Solaris
- Altre versioni UNIX
- NetWare
- Mac
- OS/2
- Open VMS Alpha
- Open VMS Vax
- Windows XP
- Windows 2000
- Winsows 2003
- Windows NT4
- Windows 98/Me
- Dos
- Linux

Figura 4: Lista delle piattaforme supportate da Sophos Anti-Virus

Supporto tecnico e customer satisfaction

Una delle differenze più significative tra i produttori di soluzioni antivirus è il supporto tecnico in-house. Il supporto tecnico di Sophos viene offerto 24 ore al giorno, 7 giorni alla settimana, 365 giorni all'anno a tutti i clienti, senza costi aggiuntivi. Alcuni produttori,

addirittura, danno il supporto tecnico in outsourcing, con il risultato che il personale di supporto non ha accesso diretto ai team di sviluppo del prodotto, che si rivelano spesso decisivi per la rapida risoluzione di un problema. Il supporto di Sophos, invece, viene offerto da un team interno di esperti, che opera nelle varie filiali in tutto il mondo, e possiede una conoscenza approfondita dei prodotti. Il successo di questa filosofia si riflette nei giudizi positivi ricevuti dal supporto tecnico di Sophos da parte di molti organismi indipendenti (per maggiori informazioni, visitare http://www.sophos.com/products/reviews/).

Information Security Magazine: La storia di copertina del numero di ottobre 2004 ha giudicato il supporto clienti di Sophos come il migliore: "Nel complesso, Sophos, che considera il supporto clienti come la pietra angolare del proprio business, è risultata la migliore".

Computing ImageTrack Survey: Per il secondo anno consecutivo, Sophos è stata giudicata "Vendor of the Year" nella categoria Security del sondaggio sulla customer satisfaction Computing ImageTrack 2004.

PC Pro Magazine: "Per il supporto che si riceve, che non è secondo a nessun altro, la scelta obbligata è Sophos...scansione antivirus performante per la rete" (Marzo 2005).

Facilità di gestione

Per offrire una protezione antivirus eccellente, è necessario che un prodotto non solo rilevi i virus in modo efficace e tempestivo, ma che sia anche facile da configurare e da mantenere. Il personale IT desidera di solito dei prodotti di sicurezza "chiavi in mano". Poiché l'antivirus è una componente cruciale dell'infrastruttura di sicurezza di un'azienda, è essenziale che il tempo necessario per la configurazione iniziale sia minimo. Ma, soprattutto, è importante che le risorse impiegate per la gestione e la distribuzione tempestiva degli aggiornamenti siano minime.

Alcuni produttori offrono tool di gestione che, sebbene pubblicizzati come ricchi di funzionalità, finiscono spesso con l'essere un lusso inutile per il cliente. Ciò è dovuto spesso alla complessità del tool di gestione, e alle difficoltà legate alla configurazione iniziale e alla gestione ordinaria, che può condurre ad investimenti ulteriori nell'acquisto di hardware per eseguire i tool di gestione e nell'assunzione di personale extra da dedicare alla messa in opera della soluzione. Ne risulta che i clienti accantonano il prodotto quando non hanno né il tempo, né la pazienza richiesti dallo stesso.

Con Sophos questo inconveniente non esiste, perché i prodotti offrono funzionalità di gestione intuitive tramite Enterprise Console™, che richiede un tempo e uno sforzo minimi. Il focus unico di Sophos è costituito da soluzioni antivirus per le aziende che rispondono alle esigenze complesse degli amministratori di rete. Sophos Anti-Virus utilizza EM Library™, che esegue l'aggiornamento automatico della rete con gli aggiornamenti delle definizioni dei virus su un'ampia gamma di piattaforme (dai sistemi operativi Windows e Mac, a Linux e UNIX), sia ad orari prestabiliti, sia su richiesta. Persino i computer degli utenti remoti e mobili vengono protetti e aggiornati in modo automatico.

Riepilogo

Tutti e sei i fattori esposti influiscono in vari modi sul fattore principale da considerare nella valutazione della protezione antivirus – il TCO (Total cost of ownership). La misurazione del TCO per i produttori e le loro soluzioni aiuta a comprendere la redditività di ogni soluzione.

Esistono altri fattori che giocano un ruolo nel calcolo del TCO, tra i quali i più ovvi sono il costo della licenza e i costi del supporto tecnico. Le aziende, tuttavia, si rendono sempre più conto che persino i costi notevoli della licenza e del supporto rappresentano spesso soltanto una piccola parte del TCO di un prodotto antivirus.

Prendendo attentamente in esame il TCO e certi aspetti, come l'upgrade della piattaforma, i costi della banda, il dispendio amministrativo, la gestione delle emergenze virus e le richieste al supporto tecnico, risulta palese che esistono differenze più o meno significative tra i vari produttori di antivirus e tra le soluzioni offerte. Per esempio, uno dei riconoscimenti di recente attribuiti a Sophos, il Gold Award nella categoria Anti-Virus Products of the Year di Information Security Magazine, ha valutato 1.239 prodotti in 13 categorie diverse, giungendo al seguente risultato: "Sophos non solo è il vincitore del Gold Award, ma impone gli standard nel settore degli antivirus". Se valutato alla luce dei vari fattori discussi in questo documento, Sophos Anti-Virus dimostra di essere la soluzione più vantaggiosa e con il TCO più basso, nonché la protezione migliore per un numero di piattaforme superiore a quello di qualsiasi altro produttore di soluzioni antivirus sul mercato.

Boston, USA • Magonza, Germania • Milano, Italia • Oxford, UK • Parigi, Francia
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Giappone

SOPHOS
www.sophos.it