Astaro OrangePaper

L'approccio tutto in uno alla sicurezza sul web

Benefici per le piccole e medie imprese

Autori:

Udo Kerst
Senior Product Manager

Eric Bégoc
Product Manager

Data: 10-04- 2008

Sommario **Pag.**

Sintesi dell'offerta

L'accesso al web dei dipendenti, sotto vari aspetti, mette a dura prova le capacità degli amministratori dei sistemi informatici e comporta rischi specifici per la sicurezza. Nonostante l'implementazione di tecniche di sicurezza sofisticate in ambito aziendale per scongiurare il rischio d'intrusioni indesiderate nella rete, gli hacker e gli esperti dello spionaggio informatico riescono comunque a trovare nuovi espedienti per immettere nel sistema immense quantità di malware, ad esempio inducendo gli utenti della rete a scaricare pacchetti di file infetti nelle loro transazioni su web. Un accesso al web senza restrizioni può inoltre assorbire notevoli risorse di rete ed aprire canali di comunicazione indesiderati, tramite i sistemi di messaggistica istantanea e gli scambi di software peer-to-peer. Per scongiurare i problemi connessi all'accesso al web, molte piccole e medie imprese riconoscono oggi i vantaggi insiti in una soluzione tutto in uno implementabile con un gateway web sicuro.

# # #

Introduzione

Nel ciberspazio nulla è statico. Dal giorno in cui fu effettuato il primo esperimento d'invio di un pacchetto dati da un laboratorio all'altro, l'infrastruttura che ha dato vita a Internet e, successivamente, al web ha subito costanti e graduali variazioni e adattamenti. Altrettanto è avvenuto per le misure di sicurezza sul web. Gli amministratori dei sistemi informatici, per permettere alle rispettive aziende di godere appieno dei benefici offerti da una rete globale di comunicazione, hanno dovuto combattere una serie incessante di attacchi sempre più sofisticati: per loro, quindi, il termine *vigilanza esterna* indica qualcosa di più che semplice retorica. Peraltro, anche quando si siano individuate e neutralizzate talune minacce, se ne palesano altre, magari più insidiose, per le quali le PMI potrebbero non disporre internamente di quel know-how necessario ad identificarle e contrastarle, in un panorama di sicurezza in rapido cambiamento.

Adattarsi alla natura mutevole delle minacce alla sicurezza significa innanzitutto individuare le vie di diffusione dei maggiori rischi, le transazioni che risultano maggiormente esposte a furti di dati o che rendono il sistema più vulnerabile, i meccanismi potenziali con i quali gli hacker o, più in generale, gli "in-

trusi" possono accedere alle informazioni interne. Altrettanto importanti sono l'identificazione e la prevenzione delle attività con le quali lo stesso personale di un'azienda potrebbe rendersi responsabile di un uso improprio delle risorse di rete, accedere ad informazioni vietate dalle vigenti leggi sulla tutela dei minori o da politiche aziendali, ovvero esporre inavvertitamente altri utenti della rete a virus o malware in circolazione. Una soluzione di *web security* può essere ritenuta più o meno valida in base all'efficacia con cui permette di perseguire questi obiettivi, senza però interferire con l'attività aziendale o comportare ulteriori inconvenienti, aggravi o disagi a carico del personale, dei soci o dei clienti di una data azienda.

Sono oggi disponibili svariati approcci alla sicurezza sul web, dalla protezione dei punti terminali, con l'utilizzo di software client, al consolidamento del firewall in uso con ulteriori funzionalità di gateway, atte a scongiurare i rischi emergenti. Il presente documento descrive i vantaggi offerti da un approccio centralizzato, implementabile con un gateway di sicurezza tutto in uno, in grado anche di potenziare ed integrare le misure di protezione esistenti. L'uso di strumenti appositamente sviluppati per contrastare le maggiori criticità attuali di accesso al web, applicati uniformemente in tutta l'azienda, consente notevoli vantaggi rispetto alle soluzioni su base client, che non garantiscono un livello altrettanto omogeneo di protezione o possono essere aggirate dagli stessi utenti. Questo documento illustra inoltre i vantaggi insiti nell'unificazione dei meccanismi di *web security* in un singolo dispositivo hardware, di facile installazione oppure, in alternativa, nell'implementazione di una vantaggiosa *appliance* virtuale monocomponente (su base VMware). Siamo infatti convinti che la realizzazione e il mantenimento in vigore di misure di *web security* possano rivelarsi attività onerose ed assorbire notevoli risorse, se implementate in modo frammentato e senza un opportuno coordinamento.

Il cambiamento: l'unica costante inconfutabile

Gli esperti dello spionaggio informatico sono creativi

Internet è oggi uno strumento indispensabile per espandere le possibilità di business. Tuttavia, con l'estensione mondiale della rete, le imprese sono oggi esposte a un numero crescente di minacce e vulnerabilità che, qualora non contrastate, finirebbero per negare i vantaggi di un modello di business "aperto". Gli amministratori e i gestori delle reti aziendali avranno senz'altro constatato che le tecnologie oggi disponibili per combattere le vulnerabilità di rete sono necessariamente in continuo cambiamento al fine di far fronte all'inventiva degli esperti dello spionaggio informatico, che riescono ad aggirare

le misure di sicurezza in modi sempre più innovativi. Peraltro, la disponibilità della rete è compromessa anche internamente da attività quali scaricare software contenente virus e worm o l'eccessivo traffico dovuto all'uso di siti di condivisione file o allo scambio di dati peer-to-peer, con la conseguente riduzione della velocità di rete.

Vulnerabilità dei server e dei programmi di navigazione

La svolta segnata dalle tecniche di hacking, che oggi destano maggiore interesse per la loro pericolosità, è il "drive-by malware", una forma di attacco "fianco a fianco" che consiste nel rendere complici gli utenti di una rete nell'infettare la stessa con le loro attività di navigazione. Questa tattica è stata escogitata a fronte delle più sofisticate misure di sicurezza oggi disponibili per neutralizzare gli attacchi di rifiuto di servizio (DOS) o le intrusioni forzate nella rete. Oggi gli hacker sono più subdoli: allettano gli utenti ad operare sui rispettivi terminali in modo da esporli a rischi, ad esempio cliccando su link ipertestuali per accedere a cartoline elettroniche o navigando semplicemente in una pagina web maligna, contenente codici di worm, virus, spyware o malware.

"L'entità del drive-by malware è significativa"

L'organo *Network World* cita uno studio di Google del 2007, in cui viene valutata la pericolosità dei download di drive-by malware[1] e, in particolare, si afferma che molti siti apparentemente benigni (siti di benessere, arte, spettacolo o relazioni sociali) sono diventati strumenti di distribuzione del malware. I siti per adulti sono ugualmente rappresentati in una percentuale elevata dei casi esaminati, la rilevazione più agghiacciante è però l'elevata incidenza di siti apparentemente innocui che sono stati appositamente manipolati dagli hacker per essere trasformati in nodi di distribuzione malware. Un metodo di manipolazione è quello di sfruttare le vulnerabilità di sicurezza dei server; lo studio di Google rileva infatti che il 38,1 dei server Apache e il 39,9 percento dei server con supporto di script PHP sono versioni con noti difetti di sicurezza. Lo studio conclude affermando che l'entità del drive-by malware è *significativa*.

[1] "Google says the scope of drive-by malware is 'significant'", articolo pubblicato su http://www.networkworld.com/newsletters/techexec/2008/0303techexec1.html

L'analista di sicurezza Mike Montecillo, della società di consulenza Enterprise Management Associates (www.enterprisemanagement.com), punta il dito contro il browser web, indicandolo come fonte primaria di vulnerabilità[2] nelle strategie di sicurezza aziendali. Secondo lo studioso, la maggior parte delle imprese mette a disposizione dei propri dipendenti tutte le funzionalità di navigazione browser, senza però prestare particolare attenzione ai rischi che la navigazione comporta e che possono essere sfruttati dagli hacker tramite applicazioni di comune diffusione, come Flash, ActiveX, QuickTime, Java e JavaScript. Ciascuna di queste componenti del browser rappresentano un canale potenzialmente sfruttabile per diffondere malware sulla rete.

"Ogni singolo sito web è un potenziale host di codici maligni. Infatti gli hacker potrebbero potenzialmente sfruttare anche i siti più legittimi come mezzo d'intrusione in migliaia di computer, senza temere interventi punitivi" afferma Montecillo. "Il numero dei siti maligni e delle vulnerabilità dovute alla navigazione, decisamente lesive e dannose per un'azienda, è potenzialmente infinito."

Per questo motivo, precisa Montecillo, molti professionisti di sicurezza informatica si affidano oggi a soluzioni di filtraggio rigoroso delle URL come misura di protezione indispensabile per la navigazione. Bloccando siti che non hanno attinenza con l'attività aziendale ordinaria, si riducono notevolmente le opportunità di violazioni della sicurezza durante la navigazione. Oltre al filtraggio, Montecillo raccomanda anche l'installazione di software anti-malware ed il filtraggio automatico dei codici per rafforzare ulteriormente le protezioni di sicurezza associate al browser.

Le nuove minacce di Skype, della messaggistica istantanea e delle applicazioni peer-to-peer

Controllare l'uso di Skype è un bel grattacapo per ogni amministratore

Un altro problema sempre più significativo deriva dalla proliferazione di applicazioni di messaggistica istantanea (IM) e di scambio file peer-to-peer (P2P). I frodatori, che utilizzano le falle di sicurezza negli applicativi di Voice-over-IP come Skype, a volte creano disagi come addebiti fraudolenti e compromissione delle pratiche commerciali. Questi strumenti di comunicazione utilizzati fra i

[2] "EMA Points to Web Browsers as Emerging IT Security Threat"; articolo pubblicato su http://www.mywire.com/pubs/PRNewswire/2008/02/26/5764914

dipendenti di un'azienda possono rivelarsi di difficile, se non impossibile, regolamentazione senza una forma di controllo centralizzato sul traffico web.
Gli utenti spesso si sentono autorizzati ad installare qualsiasi tipo di applicativo da loro preferito sulla propria postazione di lavoro, senza curarsi delle politiche o prassi aziendali. È indubbio che vi sono applicativi IM o P2P in grado di fornire a un'azienda un valore aggiunto, ciononostante gli amministratori informatici devono poter disporre di un sistema in grado di regolamentare e controllare l'acceso degli utenti in modo centralizzato, onde bloccare gli applicativi off-limits e consentire invece il libero accesso ad applicativi che offrono un valore aggiunto per l'azienda e sono usati dal personale per finalità lecite.
Ad esempio, molte imprese utilizzano BitTorrent come mezzo vantaggioso per lo scambio di file di grandi dimensioni o per il download di software. In tal caso, gli amministratori utilizzeranno un apposito meccanismo che consentirà l'accesso legittimo dei dipendenti a BitTorrent, ma negherà l'accesso ad altri applicativi ritenuti rischiosi o inadeguati.

Problematiche di comunicazione per il personale

L'uso equilibrato della banda di rete non è più una prerogativa riservata alle grandi imprese

L'accesso al web del personale ha i suoi pro ma anche i suoi contro per le piccole e medie imprese. Infatti, lo stesso canale che i dipendenti utilizzano per le loro indagini di mercato, analisi di tendenze, comunicazioni globali con clienti e partner, o ricerche di nuovi clienti e mercati, può rappresentare un potenziale generatore di traffico e quindi di intasamento della rete. I dipendenti impegnati in attività che comportano l'incanalamento di ampi volumi di dati sulle risorse di rete finiscono per interferire con il regolare svolgimento di attività aziendali prioritarie. Insomma, benché gli applicativi di comunicazione a carattere sociale o commerciale, le telefonate Voice-over-IP, l'accesso video in streaming, la condivisione di file peer-to-peer e simili modalità d'accesso al web possono avere finalità legittime sul piano aziendale, il loro uso illimitato può impedire l'utilizzo di risorse di rete che diversamente verrebbero destinate ad usi prioritari.

La diffusione di questo tipo di applicazioni web ha registrato un incremento sostanziale e rappresenta oggi un'ulteriore sfida per gli amministratori di sistema, la cui responsabilità primaria è quella di garantire un uso equilibrato della banda di rete. In passato, meccanismi centralizzati, atti a minimizzare la disponibilità di banda per applicazioni meno importanti, erano prerogativa delle grandi imprese. Le più recenti soluzioni, tuttavia, particolarmente indicate per

le piccole e medie imprese, stanno implementando questo tipo di funzionalità per far fronte all'impennata del traffico di rete direttamente attribuibile a determinate tipologie di applicazioni web (utilizzate per scopi aziendali o personali).

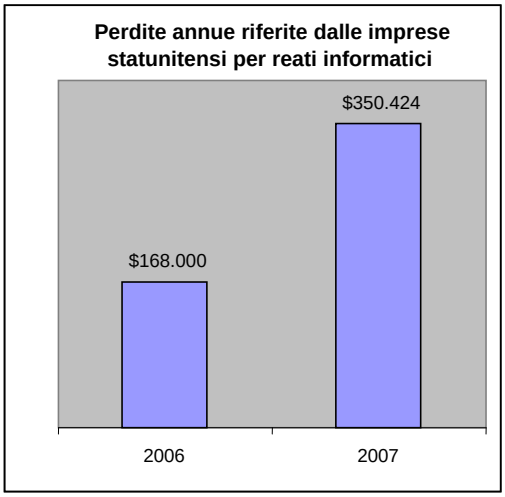
Uno studio indipendente condotto nel 2007 da Dynamic Markets[3] fornisce alcune indicazioni sul contributo dato dai dipendenti all'aumento dei rischi per la sicurezza. Lo studio esamina un campione di 750 addetti fra manager IT e dipendenti nelle PMI europee:

- Nonostante i dipendenti ammettano di trascorrere ben due ore al giorno su siti web non attinenti all'attività lavorativa, solo il 47% dei manager IT ha promosso l'adozione di sistemi di filtraggio web come forma di tutela contro le minacce di attacchi esterni.
- Poco meno di un terzo dei dipendenti confessa di accedere di frequente a siti ad alto rischio potenziale, inclusi quelli di condivisione file peer-to-peer e di download gratuito di software. La stragrande maggioranza di questi dipendenti (66%) dichiara che la loro azienda ha adottato misure di protezione contro le minacce alla sicurezza provenienti da Internet.
- A fronte di una minoranza di manager IT del campione (17%) che ritiene che le PMI necessitino di misure di sicurezza meno rigorose rispetto a quelle delle grandi imprese (dati i livelli minimi di rischio), ben il 71% ritiene invece che le dimensioni di un'impresa non contino e che quindi le PMI abbiano bisogno di un livello di protezione pari a quello delle grandi imprese.

[3] "European SMB Employees Surf for Two Hours a Day, Yet IT Managers Pass The Buck on Security"; http://newsblaze.com/story/20070823012132000002.we/topstory.html

I costi di una sicurezza su web inefficace

I virus non sono più la causa primaria di perdite finanziarie



Uno studio del 2007 condotto dal Computer Security Institute[4], in cui si quantificano le perdite finanziarie delle imprese statunitensi nel precedente anno, rileva un netto incremento delle perdite medie per impresa, da 168.000 $ nel 2006 a 350.424 $ nel 2007. Una delle cause più significative di queste perdite è l'intrusione di estranei nel sistema aziendale. Quasi un quinto degli intervistati afferma di aver subito un attacco di malware in azienda. Un'altra causa di perdite lamentata riguarda gli abusi commessi dai dipendenti nell'utilizzo del servizio di e-mail o nell'accesso alla rete. Nella casistica raccolta sui problemi di sicurezza, il traffico illecito di materiale pornografico o il download di software pirata ha un'incidenza più significativa (59% del totale) rispetto ai virus (52%).

Alla luce di questi risultati, Robert Richardson, amministratore del Computer Security Institute afferma: "Mentre gli esperti del settore discutono concitatamente in merito alla crescente sofisticazione degli attacchi informatici, circa duecento intervistati lamentano di aver registrato perdite molto più consistenti lo scorso anno. Un dato che ci induce sempre più a pensare, alla luce dei risultati dell'anno in esame, che l'impennata di attacchi si stia delineando come una reale impennata di perdite".

La versione integrale dello studio è scaricabile dal sito: www.gocsi.com.

[4] "2007 CSI Computer Crime and Security Survey Shows Average Cyber-Losses Jumping After Five-Year Decline"; http://www.gocsi.com/press/20070913.jhtml

I benefici insiti in un approccio basato sulle appliance

Le piccole e medie imprese riescono ad ottenere il massimo grado di efficienza, nei rispettivi processi aziendali, quando riescono a consolidare e a snellire le loro funzionalità in settori chiave, come la sicurezza sul web, in modo da consentire una gestione diretta, una facile supervisione, una minima manutenzione ordinaria ed un semplice processo di aggiornamento. La crescente diffusione degli approcci basati sulle "appliance" (dispositivi unificati di sicurezza rete) dimostra l'indubbia efficacia di questo modello nella soddisfazione dei criteri prefissati.

Un'appliance di sicurezza può essere costruita e implementata in uno dei tre seguenti tipi di soluzione o "pacchetti":

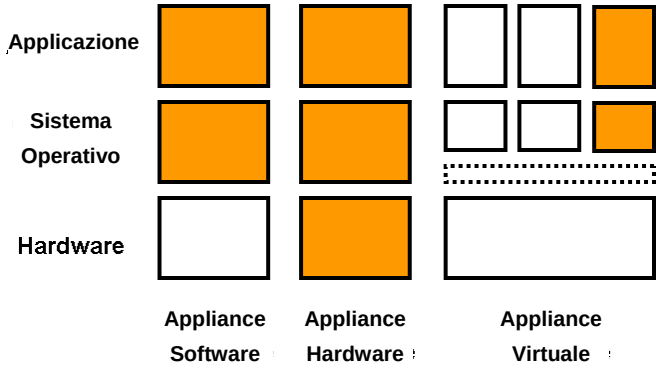


Fig. 1: tre modelli d'implementazione di un'appliance di sicurezza

- **Appliance software**: le funzionalità della soluzione di sicurezza si ottengono con un unico software image, integrato all'interno del sistema operativo e di tutte le applicazioni richieste, ai fini di una rapida installazione su un PC o server dedicato. Questa soluzione permette una più rapida ed agevole implementazione di quanto non avvenga per applicazioni software che richiedono un sistema operativo separato preinstallato.
- **Appliance hardware**: nella rete aziendale viene integrato un dispositivo hardware, con software e sistema operativo preinstallati, di rapida configurazione ai fini del funzionamento. Questa alternativa spesso rappresenta il metodo più rapido per integrare in rete le funzionalità di una soluzione di sicurezza, con un'incidenza minima d'incompatibilità o problemi d'implementazione.

- **Appliance virtuale**: l'appliance virtuale risulta dalla combinazione di tutti le applicazioni software richieste, incluso il sistema operativo, opportunamente preinstallati, preconfigurati e concepiti per essere eseguiti contestualmente ad altre appliance virtuali in un ambiente virtuale, ad esempio di tipo VMware.

Questo approccio globale nella concezione di soluzioni di sicurezza presenta tutti i vantaggi derivanti dal consolidamento della protezione necessaria in un punto chiave di vulnerabilità. Ad esempio, Astaro Web Gateway implementa una suddivisione fra le informazioni a flusso libero della navigazione Internet e l'infrastruttura di rete protetta dal firewall aziendale interno. Grazie al suo funzionamento in combinazione con il firewall, questo gateway di sicurezza è in grado di filtrare i contenuti web, di supervisionare e controllare l'uso di applicazioni web, di prioritarizzare l'uso della banda in base all'applicazione e infine di proteggere la rete interna dagli attacchi di malware in arrivo.

I benefici della virtualizzazione

La virtualizzazione è diventata la pratica più diffusa per avvantaggiarsi appieno delle risorse server disponibili, che normalmente sono sotto-utilizzate nella maggior parte delle imprese. Un'appliance virtuale preconfezionata con la funzione di plugin consente di ridurre ai minimi termini le problematiche d'installazione e configurazione. Inoltre, il set-up è il più spesso agevole, simile a quello richiesto per l'installazione di un dispositivo hardware.

Un altro beneficio insito nell'implementazione di un'appliance virtuale è dato dal risparmio di costi e di elettricità associato alla virtualizzazione. Le risorse server disponibili sono usate in modo molto più efficiente, pari quasi al 100% dell'utilizzo conseguibile con l'uso di server separati con diversi ambienti e sistemi operativi installati nella sala server. Ciò comporta un costo energetico sostanzialmente ridotto (in quanto sono necessari meno server), con l'ulteriore vantaggio per l'azienda di minimizzare l'uso del sistema di raffreddamento nella sala server. Mentre si diffonde sempre più l'adozione di misure d'informatica verde per ridurre il fabbisogno energetico e contrastare il fenomeno del surriscaldamento globale, prodotti come l'appliance virtuale Astaro Web Gateway contribuiscono a ridurre la quantità di anidride carbonica attribuibile all'informatica aziendale[5].

[5] Astaro aderisce anche alla Green Grid, un consorzio globale dedicato al progresso dell'efficienza energetica nei centri di calcolo e nelle reti aziendali ecocompatibili.

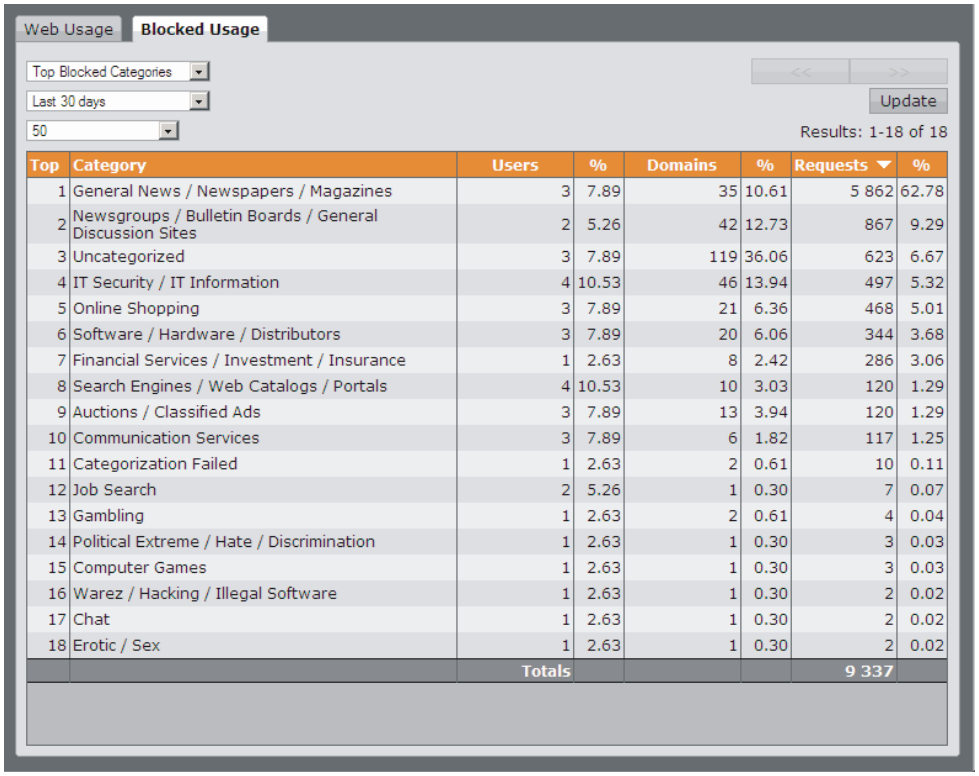
La centralizzazione delle funzionalità di sicurezza e gestione

Come già evidenziato negli esempi e dati riportati nel presente documento, gli amministratori di rete spesso non dispongono degli strumenti e delle tecnologie che consentirebbero loro di supervisionare le transazioni aziendali di accesso al web, con il conseguente rischio di aprire le porte a numerosi scenari aggiuntivi di minacce e canali di comunicazione indesiderati in grado di aggirare le normali protezioni firewall. Le soluzioni installabili su postazioni client possono sì garantire una qualche forma di protezione, ma il loro uso risulta di difficile gestione e rintracciabilità. In un'organizzazione aziendale caratterizzata da numerosi terminali, o anche quando questi sono presenti in numero relativamente contenuto, l'amministratore che tenti di procedere all'installazione di nuove patch o aggiornamenti software per tutelare la sicurezza del sistema si troverà di fronte a un'impresa titanica e senza fine. Di fatti è noto che gli stessi dipendenti possono talvolta bypassare le protezioni esistenti, disabilitando il software di sicurezza o ignorando semplicemente gli inviti a loro rivolti dagli amministratori di scaricare patch ed aggiornamenti periodici.

Il modo migliore per contrastare le svariate minacce associate all'accesso al web è di consolidare le funzionalità necessarie in una soluzione tutto in uno, su base gateway, che operi in combinazione con il firewall esistente. L'amministratore di rete avrà un'immediata supervisione e controllo del traffico web in entrata e in uscita, con possibilità di installare selettivamente opportuni filtri, monitor e controlli di flusso per regolamentare il traffico in modo sicuro e ordinato sull'intero sistema.

Per sua stessa natura, una soluzione di sicurezza web unificata e centralizzata soddisfa un altro requisito degli amministratori di rete: offre un metodo trasparente, universalmente implementato per garantire il massimo grado di conformità con la disciplina di restrizione accesso a certe tipologie di contenuto. È il caso, ad esempio, delle scuole e degli istituti di formazione, che per legge sono tenuti ad impedire agli utenti minorenni del web di visualizzare contenuti per adulti. Una soluzione di *web security* con filtri di controllo permette quindi una rigorosa osservanza delle principali disposizioni di legge, locali o nazionali, bloccando in modo efficace l'accesso a siti ritenuti inadeguati.

Tuttavia, per poter documentare l'efficacia dei controlli installati, una simile soluzione deve prevedere delle funzionalità estese di registro e reportistica, come illustrate nel seguente diagramma.



Web Usage | **Blocked Usage**

Top Blocked Categories | Last 30 days | 50 | Update | Results: 1-18 of 18

Top	Category	Users	%	Domains	%	Requests	%
1	General News / Newspapers / Magazines	3	7.89	35	10.61	5 862	62.78
2	Newsgroups / Bulletin Boards / General Discussion Sites	2	5.26	42	12.73	867	9.29
3	Uncategorized	3	7.89	119	36.06	623	6.67
4	IT Security / IT Information	4	10.53	46	13.94	497	5.32
5	Online Shopping	3	7.89	21	6.36	468	5.01
6	Software / Hardware / Distributors	3	7.89	20	6.06	344	3.68
7	Financial Services / Investment / Insurance	1	2.63	8	2.42	286	3.06
8	Search Engines / Web Catalogs / Portals	4	10.53	10	3.03	120	1.29
9	Auctions / Classified Ads	3	7.89	13	3.94	120	1.29
10	Communication Services	3	7.89	6	1.82	117	1.25
11	Categorization Failed	1	2.63	2	0.61	10	0.11
12	Job Search	2	5.26	1	0.30	7	0.07
13	Gambling	1	2.63	2	0.61	4	0.04
14	Political Extreme / Hate / Discrimination	1	2.63	1	0.30	3	0.03
15	Computer Games	1	2.63	1	0.30	3	0.03
16	Warez / Hacking / Illegal Software	1	2.63	1	0.30	2	0.02
17	Chat	1	2.63	1	0.30	2	0.02
18	Erotic / Sex	1	2.63	1	0.30	2	0.02
		Totals				9 337	

Fig. 2: report di filtraggio URL di Astaro Web Gateway

Riportiamo di seguito un passaggio del rapporto tecnico Gartner 2007, "Magic Quadrant for Secure Web Gateway 2007[6]":

> "Un gateway web sicuro (si veda l'articolo "Introducing the Secure Web Gateway") è una soluzione in grado di filtrare software/malware indesiderato proveniente da traffico Web/Internet generato dagli utenti e quindi di assicurare la conformità con le vigenti disposizioni normative ed aziendali. Per conseguire simili finalità, il gateway dovrà prevedere, come requisito minimo, funzionalità di filtraggio URL, individuazione e filtraggio di codici maligni e controlli implementati sulle più diffuse applicazioni su base web, come la messaggistica istantanea (IM) e Skype."

Il rapporto inoltre conclude:

> "Nessun prodotto è in grado d'implementare, in una stessa unità, tutte le categorie funzionali, pertanto gli acquirenti dovranno decisamente fare alcune rinunce".

Nella loro attività di sviluppo prodotti, gli sviluppatori di software Astaro si sono impegnati nella realizzazione di una soluzione onnicomprensiva ed integrata, in grado di soddisfare le esigenze delle piccole e medie imprese. Le specifiche di progettazione di Astaro Web Gateway prevedono i seguenti obiettivi primari:

- integrazione di meccanismi in grado di impedire al malware d'infettare la rete;
- regolamentazione dell'uso delle applicazioni che comportano la condivisione di file o la comunicazione fra gli utenti;
- limitazione dell'accesso ad Internet per utilizzi espressamente autorizzati dall'azienda e consentiti dalla legge;
- utilizzo della capacità di banda per applicazioni aziendali fondamentali, in via prioritaria rispetto agli utilizzi di minore importanza.

[6] Firstbrook, Peter, Lawrence Orans e Araqbella Hallawell. "Magic Quadrant for Secure Web Gateway", Gartner, giugno 2007.

Questa funzionalità, integrata nella versione di Astaro Web Gateway uscita all'inizio del 2008, permette alle aziende di soddisfare appieno i requisiti di *web security* con una singola soluzione tutto in uno.

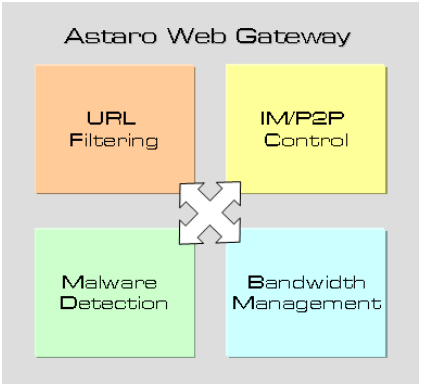


Fig. 3: Astaro Web Gateway

Risorse e costi della sicurezza

A differenza delle grandi imprese, le PMI spesso non dispongono di un consistente staff interno preposto alle problematiche di sicurezza. Lo stesso personale incaricato di rispondere alle richieste di supporto degli utenti finali spesso deve valutare e implementare le soluzioni di sicurezza aziendali, oltre a provvedere alla manutenzione dell'hardware e del software di sicurezza in uso. Misure di sicurezza complesse, che richiedono il monitoraggio individuale delle configurazioni di utente e la valutazione dell'effettiva installazione di patch aggiornate sui browser, di software antivirus e di firewall postazione per postazione risultano di difficile controllo e aggiornamento periodici. Se è vero che simili forme di protezione si rivelano utili e, in taluni casi, necessarie, è altrettanto indispensabile predisporre una prima linea, efficace, di difesa, tale da potenziare la tradizionale protezione firewall con ulteriori strumenti in grado di garantire una *web security* completa.

Astaro ha quindi concepito Astaro Web Gateway per le piccole e medie imprese, per le quali risulta indispensabile l'adozione di misure di sicurezza web a tutto tondo, in grado di potenziare le protezioni esistenti, senza però disporre dell'esperienza o delle risorse di personale necessarie ad installare una miriade di soluzioni postazione per postazione. Anche le aziende dotate di sufficienti addetti informatici riscontreranno l'indubbia utilità di un pacchetto tutto in uno, un dispositivo unificato che, più di qualsiasi altra soluzione, è in grado di soddisfare i requisiti aziendali e l'esigenza di consolidare la sicurezza, senza però dover rinunciare ai vantaggi offerti da Internet per l'attività dell'impresa.

Concentrando buona parte dell'attività di progettazione sull'utilizzabilità, l'interfaccia utente Astaro Web Gateway semplifica di gran lunga le funzioni amministrative e consente una visibilità perfetta e attualizzata dello stato di

sicurezza della rete e delle impostazioni attivate di configurazione traffico. Gli amministratori possono così valutare facilmente le vigenti politiche di sicurezza, abilitare le impostazioni atte a bloccare o filtrare le minacce più dannose conseguenti all'accesso al web e supervisionare l'intero stato di *web security* da una singola postazione centrale.

I benefici comportati da una soluzione tutto in uno

Gli amministratori di sistema che implementano una soluzione tutto in uno per la sicurezza sul web possono trarre netti vantaggi rispetto a soluzioni di filtraggio web monofunzione, più costose e complesse. Questi i benefici comportati dalla disponibilità di un controllo unificato sull'accesso al web e l'uso di Internet:

- **Efficace protezione dal malware**: i vettori di minaccia introdotti da malware, spyware, virus, worm ed altri attacchi esterni possono essere attenuati con una prima linea di difesa sostanzialmente inattaccabile.
- **Riduzione dei costi**: un'appliance centralizzata per la sicurezza web riduce le mansioni amministrative e semplifica gli interventi di manutenzione ordinaria e di aggiornamento software.
- **Conformità alla normativa vigente**: le aziende possono bloccare l'accesso a contenuto inadeguato o illegale in conformità alle politiche interne ed alla normativa vigente.
- **Maggiore produttività**: i dipendenti non perderanno preziose ore di lavoro navigando su siti non attinenti all'attività aziendale, con l'ulteriore vantaggio di diminuire il rischio d'infezioni dovute a malware inavvedutamente scaricato da siti di dubbia utilità. Sono inoltre scongiurati altri disagi, come ad esempio i sovraccarichi di rete dovuti a inopportuni flussi di bit.

Sono questi i principi cardine alla base del prodotto Astaro Web Gateway, in grado di soddisfare i requisiti degli amministratori di sistema nelle PMI.

Conclusioni

Per far fronte a categorie emergenti di minacce alla sicurezza, come gli attacchi su base web che sfruttano le vulnerabilità esistenti a livello di singolo utente o di server di rete, gli amministratori di sistema hanno bisogno di soluzioni facilmente implementabili per una protezione a tutto campo. Data la scarsa disponibilità di un livello adeguato di know-how e di risorse informatiche di sicurezza nelle piccole e medie imprese, torna particolarmente utile, per questa categoria di operatori, l'utilizzo di un'appliance unificata con funzionalità di gateway di sicurezza, atta ad implementare protezioni e controlli sull'uso della rete in modo conveniente, facilmente installabile e centralizzato. Questo approccio permette di potenziare le misure di sicurezza tradizionali offrendo, nel contempo, una protezione efficace contro le minacce esistenti e potenziali.

L'approccio tutto in uno alla sicurezza sul web offre una gestione semplificata, una maggiore uniformità di sicurezza della rete, un controllo più puntuale ed accurato dell'uso di applicazioni basate sul web a livello aziendale e una ridotta esposizione a qualsiasi tipo di minaccia web, presente o futura.

Contatti

www.astaro.com

Europa, Medio Oriente ed Africa
Astaro AG
Amalienbadstrasse 36
76227 Karlsruhe Germania
T: +49 721 255 16 0
F: +49 721 255 16 200
emea@astaro.com

Americhe
Astaro Corporation
3 New England Executive Park
Burlington, MA 01803
USA
T: +1 781 345 5000
F: +1 781 345 5100
americas@astaro.com

Asia e Pacifico
Astaro K.K.
12/F Ark Mori Building
1-12-32 Akasaka Minato-ku
Tokio 107-6012, Giappone
T: +81 3 4360 8350
apac@astaro.com