Come fronteggiare le emergenti minacce alla sicurezza causate da attacchi via Web

Un approccio multilivello per integrare le tradizionali misure di protezione

Abstract

Le aziende devono affrontare una sfida complessa per garantire la sicurezza dell'ambiente di elaborazione al quale si affidano per la propria attività. L'ambiente di elaborazione aziendale ha subito notevoli modifiche con il passare del tempo, consentendo sempre più l'accesso a molteplici contenuti e sviluppando nuove applicazioni su Internet. A causa di questa evoluzione, le aziende si trovano ora a dover affrontare molti più rischi legati alla sicurezza rispetto al passato. I recenti attacchi via Web evidenziano inequivocabilmente l'inadeguatezza della maggior parte delle misure di protezione esistenti. I firewall a livello di gateway e i software antivirus da soli non sono in grado di proteggere l'infrastruttura IT aziendale dalle minacce derivanti dai complessi codici maligni. Queste minacce emergenti pongono nuove sfide che i responsabili IT devono saper fronteggiare.

Questo documento esamina dettagliatamente alcune di queste minacce emergenti e illustra come utilizzare le soluzioni Websense per combatterle. L'offerta software di Websense consente di effettuare il filtering a più livelli — gateway Internet, rete e desktop — per offrire una soluzione completa che garantisca alle aziende una protezione totale contro le minacce alla sicurezza emergenti, trattate nel presente documento.

Websense, Inc.
World Headquarters
10240 Sorrento Valley Road
San Diego, California 92121
USA
Tel: 800.723.1166 or 858.320.8000
Fax: 858.458.2950
www.websense.com

Indice analitico

Executive summary

I recenti attacchi via Web evidenziano inequivocabilmente l'inadeguatezza della maggior parte delle misure di protezione di rete esistenti. I firewall a livello di gateway e i software antivirus da soli non sono in grado di proteggere l'infrastruttura IT dalle minacce dei codici maligni complessi. I firewall possono rilevare il traffico Web, ma la maggior parte di essi non hanno la capacità di monitorare le singole informazioni trasferite. Le soluzioni antivirus sono reattive, non preventive; sono efficaci soltanto contro minacce specifiche e offrono tale protezione limitata solo dopo che un attacco si è verificato. Le aziende hanno quindi la necessità di una soluzione che sia complementare alle soluzioni firewall e antivirus e che offra protezione a livello dei contenuti. Come descritto in questo documento, solo le soluzioni Websense sono in grado di fornire una protezione completa contro le minacce miste emergenti.

Ambiti di applicazione

La sfida

I responsabili IT sono sottoposti ad una notevole pressione nel tentativo di offrire un ambiente di relazioni aperto, collaborativo. Allo stesso tempo sono responsabili della protezione dell'azienda da perdite finanziarie e responsabilità legali che possono derivare dalle violazioni della sicurezza. Le aziende hanno risposto a questa sfida installando un insieme di prodotti e servizi di sicurezza, in genere provenienti da fornitori diversi. Queste tecnologie, quali protezione antivirus, firewall e sistemi di rilevamento delle intrusioni, sono generalmente eccellenti all'interno della propria sfera di intervento, ma non forniscono protezione sufficiente dalle minacce miste avanzate quali ad esempio Code Red e Nimda che, secondo la società di ricerca Computer Economics, hanno inciso sui costi delle aziende di tutto il mondo per 3 miliardi di dollari.

Minacce miste

Nimda e Code Red rappresentano due tra le più famose "minacce miste". Con tale definizione si designano tutte quelle applicazioni in grado di diffondersi come dei normali virus o worm, ma che hanno anche la capacità di propagarsi (o di attaccare) attraverso le vulnerabilità di sicurezza insite nei software e nei sistemi operativi. Per diffondersi, un virus deve essere costituito da uno script o da una macro, o essere contenuto in un file eseguibile e spesso i worm sono in grado di infettare la RAM o intere porzioni di disco. Un virus misto può tentare di infettare un sistema o un'applicazione attraverso il mass mailing, diffondendosi massicciamente attraverso la posta elettronica, oppure intaccando un software non aggiornato e sfruttando le falle di sicurezza non ancora scoperte.

Quando un virus "misto" arriva su un computer o un server, è in grado di distruggere o alterare i file presenti sull'hard disk. In alternativa, questi virus sono anche in grado di aprire delle backdoor, "porte" segrete che consentono al programmatore del virus di entrare nel computer infetto, oppure depositare nel sistema dei "trojan" (cavalli di Troia), piccoli file di programma all'apparenza innocui che trasformano però il computer infetto in uno "zombie". Questi microsoftware possono infatti essere risvegliati da remoto e trasformare la macchina infetta in una delle tante fonti di attacchi DDoS (distributed denial-of-service) capaci di sovraccaricare un server con una sequenza di richieste a cascata. Le minacce miste creano i cosiddetti "hacker virtuali", perché automatizzano l'entrata degli hacker in un sistema.

InformationWeek, 20 maggio 2002

Internet negli ultimi mesi è diventato molto più pericoloso per gli utenti, a causa di svariati attacchi che utilizzano il Web per lanciarsi e diffondersi nell'intera rete di computer esistenti. Alcuni nuovi exploit che in particolare sfruttano le vulnerabilità dei browser Web, compresi gli attacchi avvenuti a cavallo tra giugno e luglio 2004, evidenziano le sofisticate tecniche che gli hacker hanno sviluppato per prendersi gioco o falsificare i siti Web e come i codici maligni riescano con facilità a sottrarre nomi utente, password e altre informazioni importanti.

Gli hacker sfruttano le vulnerabilità dei browser Web per introdurre contenuti fasulli, come ad esempio dei moduli falsi per l'inserimento dei dati della propria carta di credito, sfruttando i frame di un sito sicuro. Gli utenti visitano quello che ritengono essere un sito sicuro, come una banca online o un sito di e-commerce e, mentre apparentemente il sito che visitano *sembra* essere attendibile, si tratta in realtà di una contraffazione, rendendo così gli utenti vulnerabili agli hacker che operano 'dietro le quinte'.

Apparentemente ogni giorno emergono nuove minacce sotto forma di attacchi via Internet, spyware, malicious mobile code o phishing. Tali minacce hanno inciso sui costi delle aziende di tutto il mondo per 12,5 miliardi di dollari nel 2003[1]. Le aziende non sono in grado di prevedere quando appariranno nuove minacce, da dove proverranno o quale forma potranno assumere. La soluzione consiste nel pianificare la protezione della propria azienda dalle minacce alla sicurezza nuove, emergenti e sempre più pericolose.

> *"Prepararsi ad un emergenza di questo tipo richiede un'architettura capace di individuare e bloccare automaticamente tutte le minacce, sia quelle note che quelle ancora ignote. Attualmente, le tecnologie antivirus dominanti sono quelle in grado di filtrare gli attacchi basandosi sulle firme dei file. Ma questo approccio funziona soltanto per le vulnerabilità e i codici exploit conosciuti. Considerando il tempo che intercorre tra la scoperta delle vulnerabilità e la messa in circolazione di questi codici nocivi, questo metodo non può essere sufficiente. L'obiettivo perciò è quello di dotarsi di sufficienti livelli di protezione, di modo che la violazione di uno di essi non comprometta l'intera gestione del sistema, mettendo così a repentaglio l'intera attività dell'azienda".*
>
> *Eric Litt, responsabile della sicurezza informatica presso la General Motors Corp., tratto da Computerworld, 12 luglio 2004*

Esempi di minacce emergenti

L'attacco da parte del virus *JS/Scob-A* (alias *Download.Ject* o *Toofer*) avvenuto a cavallo tra giugno e luglio 2004 ha attirato l'attenzione su questa nuova forma di minaccia in grado di usare Internet per diffondere il proprio codice maligno. I computer di ignari visitatori di alcuni siti infetti si ritrovavano a loro volta attaccati dal virus, che sfruttava a questo scopo delle vulnerabilità presenti in Internet Explorer e in alcuni server Web.

Quando i visitatori capitavano sui siti infetti subivano un reindirizzamento verso un sito russo dove, a loro insaputa e attraverso un trojan, venivano infettati da un keylogger (uno spyware in grado di registrare le battute sulla tastiera). L'insidia rimaneva presente sul computer infetto, aspettando di rilevare una visita a determinati siti (di solito siti bancari) e a quel punto il keylogger iniziava a registrare tutto quello che veniva digitato sulla tastiera. In questo modo, tutte le informazioni riservate (username, password, numero di conto) venivano trasferite direttamente al computer dell'hacker situato in Russia. Diversamente da altri attacchi verificatisi di recente, nei quali il malware si installava quando un utente rispondeva positivamente a una richiesta di installazione contenuta ad esempio in un messaggio e-mail, oppure cliccava sul link di un sito (il cosiddetto "phishing"), *tutto ciò avveniva senza che l'utente compisse nessuna azione.*

Gli ISP e le forze dell'ordine, in collaborazione con Microsoft, hanno individuato il server russo e lo hanno chiuso lo scorso 24 giugno 2004. Sebbene il sito straniero responsabile della divulgazione del virus *JS/Scob-A* sia ora definitivamente chiuso, gli amministratori IT si devono comunque impegnare per prevenire eventuali repliche di attacchi di questo tipo.

[1] Fonte: InformationWeek, 5 luglio 2004

"Il panorama della sicurezza cambia giorno per giorno e gli hacker continuano ad affinare le loro tecniche, producendo codici sempre più insidiosi che permettono di infiltrarsi nelle organizzazioni aggirando le tradizionali misure di protezione come firewall e antivirus. Recentemente, vediamo come i software di instant messaging e peer-to-peer rappresentino strade sempre più battute per diffondere attacchi. Mentre le minacce si moltiplicano, non basta allertare gli utenti, bisogna anche informarli sulle varie soluzioni di protezione in grado di tutelarli".

Lawrence Orans, analista della Gartner Research

L'esperienza di Websense

I clienti Websense che hanno utilizzato il software Websense Enterprise® Security PG™, hanno potuto usufruire di una protezione avanzata contro l'attacco a Internet verificatosi di recente da parte di *JS/Scob-A* (alias Download.Ject o Toofer). La tecnologia Websense impedisce infatti ai propri clienti di venire infettati nel periodo critico precedente al rilascio, da parte dei fornitori di prodotti antivirus, delle firme destinate a combattere gli attacchi.

Cronologia

Websense ha rilevato la minaccia *JS/Scob-A* la mattina del 24 giugno 2004. L'Internet Storm Center (SANS) ha diffuso un report che annunciava la presenza di un nuovo cavallo di Troia in Internet. Nello stesso momento, un cliente Websense ha richiesto assistenza nell'individuazione di un misterioso traffico Web verso un sito in Russia. Il giorno stesso Websense Security Labs ha effettuato delle ricerche sulla nuova minaccia alla sicurezza e ha provveduto immediatamente ad aggiungere il sito russo all'interno di Security PG.

Tabella 1. Riepilogo degli eventi

Data	Evento
24/6	Il SANS Institute rende pubblico il rapporto di un nuovo trojan. Un cliente Websense richiede assistenza nell'individuazione di traffico Web anomalo. Websense Security Lab aggiunge il sito russo all'interno di Security PG.
25/6	Le procedure di estrazione di Websense ricercano i siti infettati e ne individuano 130. Security PG effettua l'aggiornamento per includere tutti i siti e le pagine Web infettati (10.000 URL).
28/6	Websense rende pubbliche le statistiche agli utenti interessati ai temi della sicurezza: 130 domini unici risultano ancora infetti.
29/6	Le ricerche da parte di Websense individuano un nuovo exploit (IMBIG.Trojan), intercettano il codice e lo reingegnerizzano. Websense aggiorna i prodotti per bloccare i siti infetti e in seguito rende nota la scoperta agli utenti interessati ai temi della sicurezza.
5/7 6/7	Le firme antivirus per JS/Scob-A e IMBIG.Trojan sono disponibili e vengono rilasciate.

A partire dal 25 giugno Websense ha quindi aggiornato le procedure di ricerca di siti infettati da questo nuovo codice maligno stabilendo che circa 130 siti erano stati colpiti e che tutte le pagine presenti su tali siti erano infette, per un totale di oltre 10.000 URL. Websense ha quindi aggiornato i propri prodotti tramite il download notturno del database, al fine di includere tutti questi siti e pagine Web.

Il 28 giugno Websense ha divulgato agli utenti interessati ai temi della sicurezza le statistiche riguardanti le infezioni a client e server. Questa nota informativa rendeva anche noto che Websense aveva individuato più di 130 domini unici ancora infetti. Su tali siti erano in esecuzione il servizio IIS 5.0 (Internet Information Service) e il protocollo SSL e su entrambi, erano stati infettati gli URL HTTP e HTTPS. Gli indirizzi IP di questi siti si trovavano negli Stati Uniti, in Australia, in Nuova Zelanda, in Canada, in Giappone, in Spagna, nel Regno Unito e in

Norvegia.

Il 29 giugno l'analisi e la ricerca hanno individuato un altro exploit, denominato IMBIG.Trojan, che si serve anch'esso dei siti Web per infettare gli utenti. Questo nuovo exploit utilizza una diversa vulnerabilità di Internet Explorer e un BHO (Browser Help Object) che registra le sequenze di tasti premuti e li invia ad un sito Web remoto. Websense ha individuato un sito infettato e ha intercettato un esempio di codice maligno per reingegnerizzarlo. Si è così scoperto che la prima parte del codice si collegava con un altro sito laddove prelevava un altro pezzo di codice maligno. Questa nuova versione univa due applicazioni insieme. Websense ha aggiornato i propri prodotti tramite il download notturno del database, ha bloccato i siti Web infettati appena individuati e ha reso nota la scoperta agli utenti interessati ai temi della sicurezza.

> *"Personalmente ritengo che questo particolare tipo di malware rappresenti un'enorme minaccia per l'industria finanziaria su Internet. Infatti, come dimostra la proliferazione di adware e spyware, è fin troppo semplice installare dei file eseguibili sul proprio PC. Persino l'utilizzo dei famigerati BHO (le funzionalità aggiuntive del browser come pulsanti, barre di navigazione ecc.) nasconde, in modo ancora più insidioso, la possibilità che malintenzionati trafughino informazioni personali".*
>
> *Tom Liston, ricercatore del SANS Institute che ha analizzato l'attacco, tratto da eWeek.com, 29 giugno 2004*

Per molti produttori di soluzioni antivirus sono stati necessari diversi giorni prima di riuscire a rendere disponibili le firme per questi codici maligni. Durante questo periodo di tempo i clienti Websense erano comunque protetti, anche se le firme antivirus non erano state ancora rilasciate.

I tre livelli di applicazione delle policy forniti dal software Websense — gateway Internet, rete e desktop — comprendono un approccio di sicurezza multilivello che consente di proteggere gli utenti da questo nuovo tipo di minacce. Security PG blocca l'accesso da parte dei dipendenti a siti Web noti per il malicious mobile code (MMC) contenuto, ovvero siti responsabili della divulgazione dei cavalli di Troia e impedisce la trasmissione di informazioni riservate ai server non autorizzati (ad esempio il server Web in Russia). Security PG dispone inoltre di SiteWatcher™, un servizio a valore aggiunto che avvisa gli amministratori IT se il sito aziendale è stato infettato da un MMC.

> *"Gli ultimi attacchi destinati agli ambienti IT stanno diventando sempre più pericolosi e sofisticati, in grado anche di aggirare le tradizionali soluzioni antivirus. L'incertezza e il potenziale danno alla rete sono due problematiche in cima alle preoccupazioni dei professionisti della sicurezza informatica. Con Websense Enterprise Security PG e Client Policy Manager, i clienti di Websense possono impedire ai dipendenti di accedere inconsapevolmente a siti che contengono codice maligno, proteggendo così i computer e l'intera rete aziendale da eventuali attacchi e infezioni".*
>
> *Dan Hubbard, responsabile del dipartimento " Security and Technology Research" di Websense, Inc.*

Per una protezione aggiuntiva a livello desktop, Websense® Client Policy Manager™ (CPM) garantisce che i computer dei dipendenti siano protetti da MMC quando si trovano in modalità "Application Lockdown" e "Network Lockdown". La modalità Application Lockdown consente esclusivamente alle applicazioni presenti su un elenco autorizzato dall'azienda di essere eseguite sui computer dei dipendenti e, inoltre, offre una protezione efficace contro cavalli di Troia ed altre minacce provenienti da Internet come spyware. La modalità Network Lockdown impedisce alle infezioni presenti sui computer dei dipendenti di comunicare

e diffondersi attraverso la rete, proteggendo in tal modo la rete stessa, una volta colpita, da un'ulteriore diffusione di codice maligno.

> *Malgrado la presenza di firewall e di gateway antivirus, anche le singole postazioni possono diffondere virus o worm. Questo è possibile in caso di dipendenti che utilizzano i notebook, che possono infettarsi fuori dalla rete aziendale e trasmettere poi il virus all'intera LAN al momento di collegarvi il proprio computer portatile. Attraverso le falle dei sistemi operativi, anche le postazioni locali possono quindi esporre la rete aziendale all'attacco da parte di trojan, spyware e applicazioni fraudolente scaricate da Internet.*
>
> *Network Magazine, 1 luglio 2004*

In che modo Websense protegge dagli attacchi via Web

I tre livelli di applicazione delle policy da parte di Websense — gateway Internet, rete e desktop — comprendono un approccio di sicurezza multilivello che consente di proteggere dagli attacchi via Web.

Nucleo centrale di Websense Enterprise® è il Master Database, la più ampia e precisa raccolta e classificazione di siti, protocolli e applicazioni disponibile nel settore. Il Master Database di Websense comprende i siti, i protocolli e le applicazioni più frequentemente visitati sul Web e contiene oltre 8 milioni di siti classificati in più di 90 categorie e in oltre 50 lingue.

I siti vengono identificati attraverso tecniche proprietarie basate su software, compresa la funzionalità WebCatcher™, e successivamente classificati in categorie combinando procedure e tecnologie uniche con l'intervento di analisti Web. Il database viene rinnovato ogni sette ore per garantirne la massima precisione e viene aggiornato quotidianamente con aggiunte, modifiche e cancellazioni.

WebCatcher consente ai clienti di Websense Enterprise di sottoporre all'analisi di Websense gli URL non ancora classificati, vale a dire i siti Web che non appartengono a nessuna delle oltre 90 categorie di contenuti. La tecnologia unica di Websense, WebCatcher, individua i siti non classificati in base ai registri di accesso, tra centinaia di segnalazioni provenienti da clienti Websense in tutto il mondo. I siti vengono valutati, classificati e in seguito aggiunti al Master Database di Websense. Queste attività vengono svolte quotidianamente consentendo, pertanto, un perfezionamento continuo nella precisione e completezza del database.

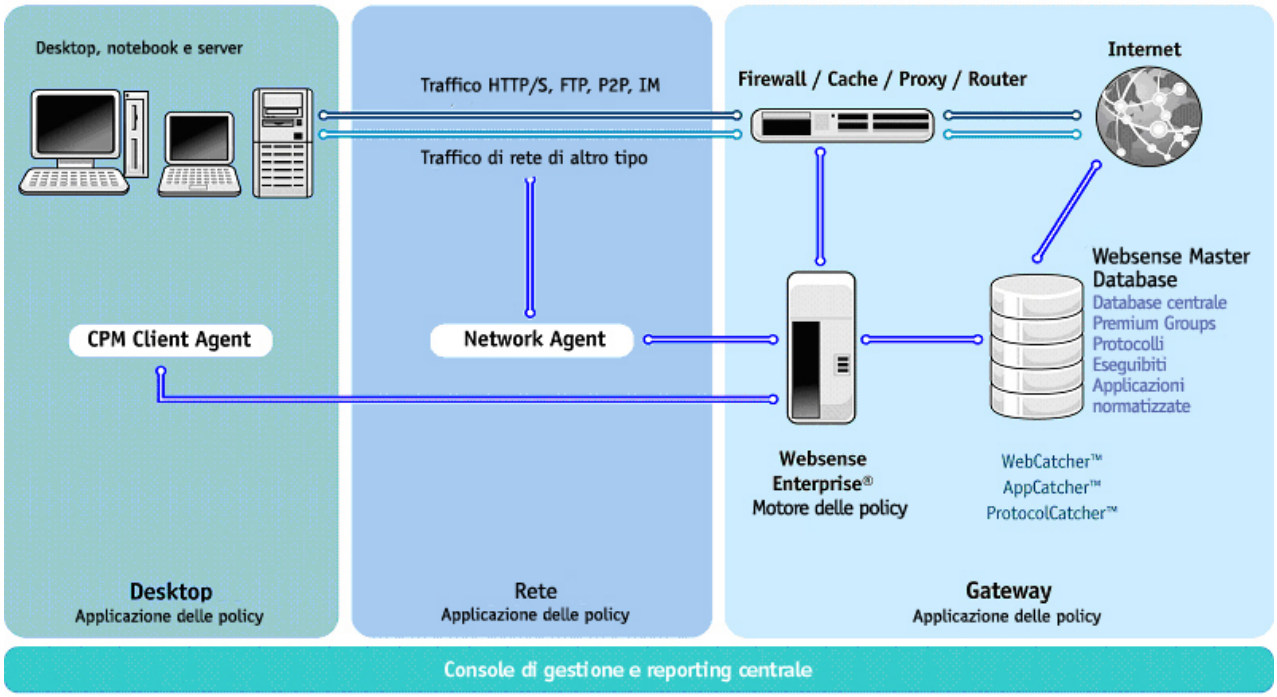

Figura 1. WebCatcher individua i siti non ancora classificati, che vengono così valutati, categorizzati e in seguito aggiunti al Master Database di Websense.

I miglioramenti apportati al database innescati dalle segnalazioni effettuate tramite WebCatcher, vengono resi disponibili a tutti i clienti Websense tramite la procedura giornaliera di download del database. In tal modo ciascun cliente può godere dei vantaggi dei modelli di navigazione globali dell'intera comunità di clienti Websense. L'intercettazione di tutti gli URL non classificati rappresenta il miglior sistema per garantire la protezione dell'accesso a Internet da parte dei dipendenti. La funzionalità WebCatcher di Websense coniuga la tecnologia di classificazione all'avanguardia con l'intervento da parte di esperti qualificati, al fine di garantire la massima precisione. Il risultato è una check list che massimizza sia l'ampiezza della copertura sia la precisione del database.

AppCatcher™, una funzionalità di CPM, garantisce che le applicazioni e gli eseguibili nuovi o non ancora classificati, avviati dai dipendenti, vengano categorizzati e aggiunti al Master Database di Websense. AppCatcher si comporta con le applicazioni come WebCatcher si comporta con gli URL. Di fatto AppCatcher assicura che Websense sia aggiornato sulle più recenti applicazioni ed eseguibili per garantire che questi siano classificati e normalizzati. Quando la funzionalità AppCatcher è abilitata, le informazioni riguardo a ciascun eseguibile sconosciuto vengono inviate automaticamente e in forma privata a Websense, dove gli analisti eseguono ricerche e lo assegnano a una categoria, eseguendo la normalizzazione[2]. Quando il server CPM scarica successivamente l'elenco aggiornato di applicazioni, le precedenti informazioni sulle applicazioni e gli eseguibili sconosciuti vengono aggiunte, consentendo in tal modo la loro classificazione e normalizzazione automatica.

[2] Il processo di normalizzazione comporta la classificazione di più eseguibili in un'unica applicazione. Ad esempio, anche se Microsoft Outlook è composto da più componenti applicativi, l'archivio CPM individua e segnala un'unica applicazione denominata "Microsoft Outlook".

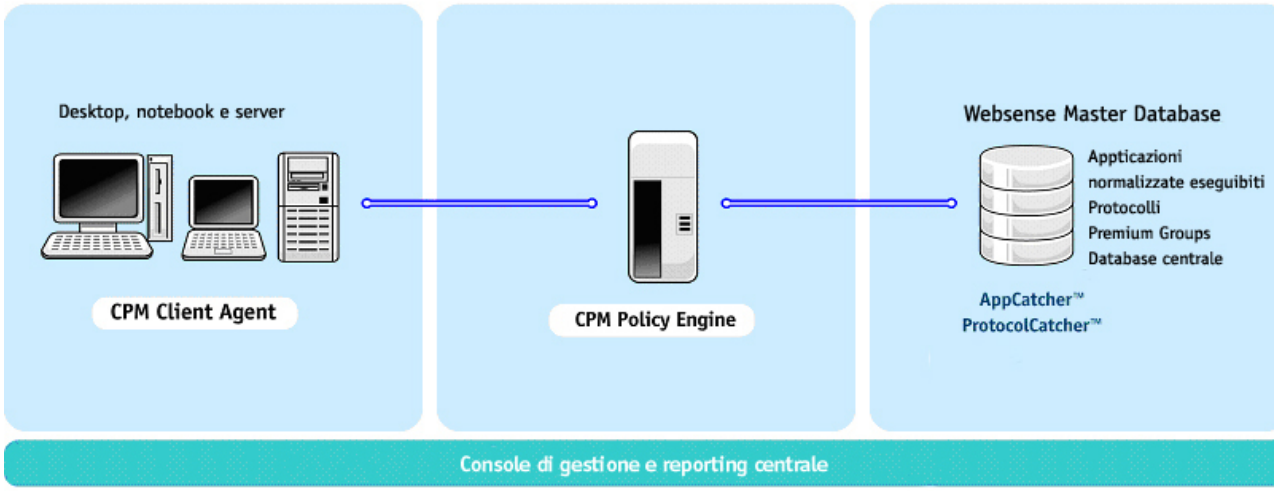

Figura 2. AppCatcher di CPM raccoglie, classifica e normalizza le applicazioni e gli eseguibili sconosciuti.

WebCatcher e AppCatcher sfruttano le tecnologie e l'esperienza di estrazione, classificazione e distribuzione a livello mondiale e sono parte di ciò che rende il software Websense Enterprise unico.

Conclusioni

Apparentemente ogni giorno emergono nuove minacce alla sicurezza, sotto forma di attacchi via Internet come quelli verificatisi di recente e descritti in precedenza, o tramite spyware, malicious mobile code o phishing. I recenti attacchi via Web evidenziano inequivocabilmente l'inadeguatezza della maggior parte delle misure di protezione di rete esistenti. I firewall a livello di gateway e i software antivirus da soli non sono in grado di proteggere l'infrastruttura IT dalle minacce dei nuovi codici maligni. Le aziende non possono prevedere da dove proverranno le nuove minacce o quale forma potranno assumere. La soluzione consiste nel pianificare in anticipo e garantire la protezione dalle minacce alla sicurezza nuove ed emergenti.

Le tradizionali misure di protezione non sono in grado di gestire in modo opportuno queste minacce emergenti. Le aziende hanno la necessità di aumentare le proprie difese di sicurezza servendosi di una soluzione che offra una reale gestione dei contenuti. I tre livelli di applicazione delle policy da parte di Websense — gateway Internet, rete e desktop — comprendono la protezione multilivello indispensabile per l'ambiente di elaborazione aziendale.

Per ulteriori informazioni e per scaricare una versione di prova gratuita e completamente funzionante valida 30 giorni, visitate il sito **www.websense.com/downloads**.

Informazioni su Websense

Websense Inc. (NASDAQ: WBSN), principale fornitore di soluzioni EIM (Employee Internet Management), consente alle aziende di ottimizzare l'utilizzo delle risorse IT da parte dei dipendenti e di ridurre minacce alla sicurezza quali instant messaging, P2P e spyware. Contribuendo a rafforzare le policy di sicurezza delle aziende a livello di gateway Internet, rete e desktop, le soluzioni Websense aumentano la produttività e la sicurezza, ottimizzano l'uso delle risorse IT e riducono il rischio di responsabilità di carattere legale. Websense protegge oltre 24.000 clienti in tutto il mondo per un totale di circa 19,8 milioni di utilizzatori. Per ulteriori informazioni, visitare il sito www.websense.com.