

IBM Express Managed Security Services per la sicurezza sul Web

Caratteristiche principali

- **Contribuisce a proteggere gli investimenti IT e la produttività dalle minacce provenienti dal Web.**
- **Sottopone a scansione il traffico sul Web alla ricerca di virus e spyware, bloccandoli prima che possano raggiungere la rete aziendale.**
- **Facilita l'applicazione delle politiche di utilizzo di Internet bloccando l'accesso ai siti Web con contenuti inappropriati.**
- **Fornisce una soluzione in hosting progettata per offrire un livello di protezione superiore a un costo totale di proprietà (TCO) inferiore.**

Contro le minacce sempre più sofisticate che affliggono le aziende

La vostra posta elettronica può già essere protetta da virus e spyware, ma l'accesso al Web è sufficientemente protetto?

Aziende e singoli utenti di Internet si trovano oggi ad affrontare minacce alla sicurezza di natura notevolmente diversa. La posta elettronica è ancora il mezzo più comune utilizzato per tentare di diffondere virus e spyware, ma questa è oggi molto più sicura che in passato. Ciò è probabilmente dovuto a due fattori: ci sono a disposizione strumenti migliori per identificare e neutralizzare le minacce e gli utenti sono più informati sulla corretta gestione dei messaggi e-mail con allegati sospetti.

In risposta a questo maggiore livello di sicurezza della posta elettronica, gli sviluppatori di virus e spyware tendono sempre di più a sfruttare i browser Web come mezzo di diffusione. Aiutati dalle abitudini di navigazione sul Web senza restrizioni di molti utenti aziendali e guidati dai possibili guadagni derivanti dal furto dei dati personali e della proprietà intellettuale, i pirati informatici e gli sviluppatori di virus appaiono motivati, creativi e irriducibili nella ricerca di nuove vulnerabilità.

A differenza delle minacce basate sulla posta elettronica, che in genere sono dirette a singole macchine e richiedono una qualche azione da parte dell'utente, le minacce alla sicurezza sul Web sono in grado di lanciare sofisticati attacchi coordinati che richiedono un contributo minimo, se non nullo, da parte dell'utente. Spyware, adware e altri software dannosi si installano spesso all'insaputa dell'utente, senza lasciare tracce, raccogliendo informazioni e compromettendo le prestazioni del sistema senza destare sospetti. Una volta installato può risultare difficile rilevare e rimuovere il software dannoso, che spesso si reinstalla ripetutamente e disattiva le misure di sicurezza. La gestione di un attacco del genere può comportare un notevole dispendio di energie per qualsiasi reparto IT.

La navigazione sul Web senza restrizioni da parte dei dipendenti può aggravare la situazione. Le aziende più oculate adottano politiche di utilizzo di Internet per contenere la navigazione improduttiva, ma, più spesso, si affidano alla buona fede dei dipendenti. Eppure, vari dati di settore indicano che una percentuale notevole dell'intera attività sul Web

delle aziende non è legata alle attività lavorative. E senza le dovute misure di protezione, anche la navigazione più innocua può portare l'utente a visualizzare contenuti inappropriati o a siti Web che agiscono come piattaforme di lancio per l'installazione di software dannosi.

Fronteggiare le sfide imposte da queste minacce è difficile per qualsiasi azienda, ma lo è ancora di più per le piccole e medie imprese che, in genere, dispongono di risorse limitate. Dato il livello di complessità, la costante evoluzione delle minacce e la grande varietà dei metodi di attacco utilizzati, il mantenimento della sicurezza sul Web richiede spesso più risorse e più attenzione di quanto i reparti IT siano in grado di offrire.

Rispondere alle minacce alla sicurezza sul Web prima che raggiungano la rete aziendale

L'approccio tradizionale alla sicurezza sul Web prevede l'installazione di software per la sicurezza a livello di desktop, oppure l'utilizzo di appliance di sicurezza a livello di rete aziendale. Il problema principale di queste soluzioni è che permettono alle minacce di raggiungere la rete aziendale; è come lasciare la porta aperta e sperare che i ladri non entrino.

La maggior parte delle soluzioni per la sicurezza tradizionali è anche difficile da configurare, monitorare e mantenere, con aggiornamenti

delle definizioni di virus e spyware che mettono a rischio la disponibilità dei sistemi, rallentando la produttività e consumando le preziose risorse del supporto IT. In genere, queste soluzioni forniscono una protezione limitata contro le epidemie improvvise – zero-hour - di software dannosi, nuovi o non rilevati, che possono attaccare i sistemi prima che sia stato possibile aggiornare le definizioni dei virus. Anche gli approcci tradizionali basati sul filtro degli URL presentano degli inconvenienti, per eccesso o per difetto, bloccando l'accesso a siti necessari oppure ignorando attività sospette da parte di URL apparentemente innocui.

La suite IBM Managed Security Services per la sicurezza sul Web è progettata per proteggere gli investimenti IT e la produttività dell'azienda, attraverso la riduzione delle minacce di spyware e virus diffuse mediante il Web e un'applicazione efficace delle politiche aziendali di utilizzo di Internet, filtrando l'accesso agli URL inappropriati o potenzialmente pericolosi. Parte della famiglia IBM Express Managed Services, questi servizi per la sicurezza sul Web sono stati creati specificamente per le medie imprese. Inoltre, trattandosi di servizi in hosting, non richiedono alcun investimento hardware o software e, una volta attivati, necessitano di una gestione minima. Il prezzo mensile si basa sul numero di utenti, per permettere alle aziende di scalare la soluzione in base alle proprie esigenze.

La suite comprende quattro opzioni di servizio:

- *Antivirus*
- *Antivirus e antispymware*
- *Filtro degli URL*
- *Antivirus, antispymware e filtro degli URL.*

Impedire a virus e spyware di raggiungere il desktop

I servizi antivirus e antispymware sono progettati per fornire una scansione in tempo reale del traffico Web in entrata e in uscita. I nostri servizi utilizzano motori di scansione antivirus e database di spyware, adware e phishing selezionati per la loro precisione e sono in grado di offrire una protezione superiore a quella ottenibile attraverso le soluzioni single vendor, difficili da realizzare internamente a causa dei costi in genere proibitivi. I servizi antivirus e antispymware di IBM analizzano rapidamente il contenuto della richiesta di una pagina Web o di un tipo di file e stabiliscono se passarla o meno al browser dell'utente finale. Le richieste inaccettabili vengono messe in quarantena ed eliminate.

I nostri servizi antivirus e antispymware non si limitano a proteggere l'infrastruttura IT dalle minacce conosciute, ma contribuiscono anche a salvaguardarla dalle attività dannose non identificate. Per mezzo di avanzate tecniche di analisi euristica, i nostri servizi sono in grado di migliorare le loro capacità nel tempo. Identificano gli schemi delle attività associate alle minacce e questo permette loro di

prevenire gli attacchi improvvisi che ormai rappresentano la maggior parte dei casi. E dal momento che i servizi analizzano le minacce sul Web al di fuori della rete aziendale, il rischio che quelle minacce possano infettare i sistemi dell'azienda è praticamente azzerato.

Inoltre, poiché i servizi monitorano anche il traffico in uscita, sono in grado di rilevare e prevenire eventuali tentativi di lanciare attacchi di virus e spyware dall'interno della rete, contribuendo a proteggere l'azienda e la reputazione del marchio. Questi servizi completi, interamente in hosting, sono progettati per richiedere il minimo intervento del reparto IT, pur offrendo all'utente un certo controllo sui servizi. Una interfaccia di amministrazione basata sul Web consente di impostare le proprie preferenze, per consentire ad esempio l'adware non invasivo, e di impostare avvisi e funzionalità di reporting.

Un accesso a Internet protetto e controllato

Il servizio di filtro degli URL di IBM Managed Security Services per la sicurezza sul Web assiste l'Azienda nell'applicazione delle politiche di utilizzo di Internet e contribuisce a garantire la conformità alle normative e legislazioni attinenti monitorando e controllando i contenuti in ingresso nella rete aziendale. Contribuisce inoltre a fare in modo che gli utenti aziendali non possano accedere accidentalmente a siti inappropriati e permette di respingere le tecniche di phishing e di spoofing, che possono portare gli utenti a rivelare inavvertitamente informazioni riservate o a installare degli spyware.

Il servizio è altamente personalizzabile e consente di impostare diverse politiche basate su categorie di URL o sui contenuti, garantendo all'Azienda un maggiore controllo e contribuendo a proteggere sia i dipendenti sia la reputazione del marchio. Il filtro degli URL permette di:

- *Applicare politiche basate su tipi di file MIME (Multipurpose Internet Mail Extensions) per limitare i tipi di file di grandi dimensioni, ad esempio audio e video.*
- *Applicare politiche basate su tipi di file specifici, quali MP3, MP4 e AAC.*
- *Controllare l'accesso a oltre 60 categorie di URL e bloccare i servizi proxy anonimi che reindirizzano il traffico verso destinazioni inappropriate.*

- *Bloccare l'accesso alla posta elettronica basata sul Web, che generalmente non è legata all'attività lavorativa e può aggirare il software antivirus e antispyware del computer in uso.*
- *Limitare l'accesso ad alcuni siti durante l'orario di lavoro e mitigare le restrizioni oltre tale orario.*
- *Configurare il servizio con impostazioni a livello di utente e di gruppo, utilizzando le informazioni esistenti sulle directory.*

A differenza della posta elettronica, per la quale un certo ritardo è tollerabile, la navigazione efficiente sul Web per scopi lavorativi richiede una velocità elevata. I servizi antivirus, antispyware e di filtro degli URL sono progettati per monitorare il traffico sul Web e reindirizzare le minacce verso l'infrastruttura protetta IBM, senza alcun ritardo rilevante per l'utente finale. Si tratta di un semplice passaggio in più nell'indirizzamento del traffico di rete; un ritardo di pochi millisecondi che può offrire all'azienda notevoli vantaggi.

Tutti i moduli di IBM Express Managed Security Services per la sicurezza sul Web sono accessibili agli amministratori tramite una interfaccia basata sul Web di facile utilizzo, che consente di modificare i servizi in base a nuove esigenze. I servizi sono progettati per integrarsi con la soluzione IBM Express Managed Services per la sicurezza e-mail.

Riduzione dei costi di protezione dell'accesso al Web

IBM Express Managed Security Services per la sicurezza sul Web offre alle aziende potenziali vantaggi interessanti. Il livello di protezione avanzato dovuto all'identificazione e alla rimozione delle minacce prima che queste possano raggiungere la rete aziendale contribuisce al raggiungimento degli obiettivi critici di business:

- *Assicurando la continuità del business*
- *Migliorando la produttività dei dipendenti*
- *Proteggendo i dati dell'azienda.*

Trattandosi di soluzioni in hosting, i servizi antivirus, antispyware e di filtro degli URL di IBM eliminano la necessità di effettuare ulteriori investimenti in hardware e software, migliorando al contempo il livello di protezione e di produttività dell'azienda e dell'infrastruttura. I moduli di IBM Express Managed Security Services per la sicurezza sul Web includono i servizi IBM Help Desk e l'accesso all'Incident Response Team di IBM, sempre pronto ad assistere i nostri clienti nella remota eventualità di una violazione della sicurezza.

Perché scegliere IBM?

Le soluzioni IBM garantiscono sicurezza e serenità. In tutto il mondo, le aziende si affidano a IBM per lo sviluppo di prodotti e servizi di sicurezza per rispondere oggi alle sfide per la sicurezza di domani. Le strutture di hosting di altissimo livello, la competenza in fatto di sicurezza e la rete di Business Partner IBM ci permettono di proteggere le funzioni di business, la reputazione e il marchio dei nostri clienti.

Ulteriori informazioni

Per ulteriori informazioni su IBM Express Managed Security Services per la sicurezza sul Web, contattare il proprio rappresentante IBM (o Business Partner IBM) oppure visitare il sito:

ibm.com/services/it



IBM Italia S.p.A.

Circonvallazione Idroscalo
20090 Segrate (MI)

La home page IBM è disponibile all'indirizzo Internet **ibm.com/it**

IBM, il logo IBM, ibm.com, ON (dispositivo a pulsante), e il logo On Demand Express Portfolio sono marchi di International Business Machines Corporation negli Stati Uniti e/o in altri paesi.

Nomi di altre società, prodotti o servizi possono essere marchi di altre società.

Ogni riferimento a prodotti, programmi o servizi IBM non implica la volontà, da parte di IBM, di rendere tali prodotti, programmi o servizi disponibili in tutti i paesi in cui IBM opera. Ogni riferimento a prodotti, programmi o servizi di IBM non implica che possano essere usati solo prodotti IBM. In sostituzione, potrà essere usato qualunque prodotto, programma o servizio funzionalmente equivalente.

Questa pubblicazione è fornita solo a titolo informativo. Le informazioni sono soggette a modifiche senza preavviso. Per informazioni aggiornate sui prodotti e servizi IBM disponibili, contattare l'ufficio vendite o il rivenditore IBM locale.

IBM non fornisce informazioni legali, economiche o di controllo né garantisce che i prodotti e i servizi forniti assicurino conformità alle leggi vigenti. Il cliente è responsabile della conformità con la normativa vigente applicabile in materia di titoli, inclusa quella nazionale.

© Copyright IBM Corporation 2006
Tutti i diritti riservati.