

## **Come innalzare il livello di protezione contro le minacce Internet più sofisticate**

Le minacce Internet proliferano ed evolvono a ritmi senza precedenti tanto che persino l'azienda più attenta può vedere le proprie difese violate da un pericolo che non era stato previsto, con il risultato che un solo passo falso può essere sufficiente per esporre l'intera attività a una serie di gravi pericoli. Consideriamo tre esempi:

### *Azienda A: La protezione "tradizionale" si rivela insufficiente*

Questa azienda ha implementato difese a prova di bomba contro minacce Internet di tipo "classico" quali virus, Trojan horse, worm e spyware. L'organizzazione ha acquisito la tecnologia di sicurezza di uno dei principali vendor del settore e mantiene regolarmente aggiornati i relativi software e abbonamenti. Di conseguenza l'azienda si ritiene ragionevolmente protetta e il suo team IT è convinto di poter dormire sonni tranquilli. Ma il sogno di un'azienda protetta si sta trasformando rapidamente in un incubo.

- Il personale mina le performance della rete attraverso podcast e download peer-to-peer irregolari di musica, video e software, in potenziale violazione delle leggi sul copyright.
- La proprietà intellettuale è posta a repentaglio attraverso messaggi e-mail spediti da addetti disattenti o scarsamente scrupolosi.
- L'Instant Messaging espone l'azienda al rischio di mancato rispetto della conformità normativa.
- Un patito del gioco d'azzardo gioca continuamente a poker online trascurando il proprio lavoro, mentre un assiduo frequentatore di siti porno aumenta i rischi di problemi con la legge.
- Incapace di garantire l'applicazione della propria policy d'impiego accettabile, l'azienda non ha modo di assicurare la produttività del personale, proteggere dagli abusi le proprie risorse di rete o evitare i gravi rischi per il business associati a tali abusi.

### *Azienda B: gli utenti mobili indeboliscono il perimetro difensivo*

Questa azienda ha innalzato la protezione a un gradino ancor più elevato. A un solido perimetro difensivo si accompagna infatti un rigido controllo mediante policy su P2P, IM, podcast e impiego del Web. Ogni problema può dunque dirsi risolto? Magari!

Il personale dell'azienda viaggia spesso per affari e lavora presso le sedi di clienti e partner, a casa, in albergo, in aeroporto, sul treno: in pratica, ovunque sia disponibile una connessione di rete. Ogni volta che operano al di fuori della rete aziendale, questi utenti espongono a loro insaputa i laptop proprio a quei tipi di malware che l'azienda si è tanto adoperata per contrastare, traghettandoli all'interno del perimetro difensivo. Dispositivi storage rimovibili non controllati, quali drive USB, rappresentano un'ulteriore fonte di minacce. E il problema si ripresenta da capo.

### *Azienda C: La minaccia della complessità*

Questa azienda ha compiuto il proprio dovere e ha implementato misure difensive di alto profilo a ogni livello, compresi gli utenti mobili e quelli non collegati. La sua infrastruttura per la protezione Internet farebbe la gioia di qualunque azienda, se soltanto non risultasse tanto costosa e complessa da amministrare e mantenere. In realtà, la soluzione di protezione resta implementata soltanto parzialmente, avendo portato al limite le risorse IT disponibili.

- Il personale IT, oberato di lavoro, non ha avuto il tempo di personalizzare la soluzione per soddisfare appieno le esigenze dell'azienda in materia di policy, rischi e conformità normativa, con la conseguenza di aver dato vita a un'implementazione generica afflitta da troppe lacune.

- Le richieste di assistenza tecnica vengono soddisfatte col ricorso a costosi servizi di consulenza aggiuntivi.
- Gli aggiornamenti segnano il passo a causa della mancanza di risorse economiche e IT.
- In considerazione di tutto il denaro e il tempo spesi l'azienda è ancora lontana dal disporre di una protezione davvero efficace. Ovviamente, una protezione deve andare oltre le apparenze per risultare effettivamente efficace. Per evitare seri rischi le aziende devono comprendere appieno la portata della sfida e affrontarla in modo appropriato, collaborando con un partner che faccia altrettanto.

### *I fattori chiave per ottenere una protezione Internet completa e conveniente*

Tecnologie e capacità difensive allo stato dell'arte sono naturalmente essenziali per implementare una protezione efficace. Le moderne minacce diversificate, che utilizzano più vettori di attacco, impongono l'impiego delle migliori contromisure possibili in ogni punto vulnerabile dell'infrastruttura, dal gateway fino ai desktop passando attraverso tutto quanto vi sta in mezzo. Ma ciò rappresenta soltanto una parte del quadro complessivo.

Le attività di ogni azienda sono uniche, così come i requisiti di protezione. In generale, l'efficacia di una soluzione per la protezione Internet dipende da sei fattori: protezione per ogni punto vulnerabile; protezione per i punti chiave della gestione; difesa proattiva; flessibilità nel deployment; personalizzazione e controllo; e valore ottimale in rapporto alle esigenze.

### *Protezione per ogni punto vulnerabile*

Poiché le moderne minacce diversificate si presentano sotto molteplici forme e attraverso molteplici canali Internet, le aziende devono implementare protezioni omogenee a livello di Web, e-mail, dispositivi mobili e client desktop. Ognuno di questi vettori deve condividere l'accesso a un database comune delle minacce in modo tale che, ad esempio, un virus possa essere riconosciuto indipendentemente dal fatto che provenga dalla posta elettronica, dalla webmail, da dispositivi storage rimovibili o da hot-spot pubblici.

Una protezione di tipo stratificato è in grado di fornire ulteriori garanzie contro questo tipo di minacce: un database delle minacce note viene integrato da tecniche euristiche e altre metodologie avanzate per filtrare le minacce sconosciute. Tecnologie di protezione e analisi condotte da esperti procedono di pari passo per identificare e bloccare le minacce emergenti. Le definizioni standard delle minacce sono integrate da definizioni specifiche per l'azienda e per il settore in cui opera, mentre alla cifratura delle informazioni si accompagna il filtraggio intelligente dei contenuti in modo da prevenire le perdite di dati. Indipendentemente dalla tipologie di rischio cui è esposta l'azienda, un approccio articolato su più strati è in grado di fornire il livello di protezione più elevato.

### *Protezione per i punti chiave della gestione*

Sulla base dell'architettura IT, dell'infrastruttura e degli obiettivi di sicurezza di un'azienda, la protezione può essere implementata a livello della rete, dei desktop oppure esternamente via Internet sotto forma di servizio on-demand. Le aziende devono valutare questo aspetto critico e, idealmente, implementare la protezione in tutti e tre i livelli. In questo modo le minacce possono essere neutralizzate indipendentemente dal luogo e dal modo in cui tentano di penetrare nell'ambiente di rete. Persino gli utenti non collegati alla rete possono essere protetti mediante applicazioni a livello di cliente oppure on-demand.

### *Difesa proattiva*

Le minacce Internet in rapida evoluzione richiedono una vigilanza costante, analisi da parte di esperti e misure preventive costantemente aggiornate. L'approccio ottimale per identificare le minacce emergenti e proteggersi da esse richiede l'unione di tecnologie allo stato dell'arte, esperti qualificati e un'infrastruttura per distribuire automaticamente la protezione aggiornata in tutto il mondo e in qualsiasi momento. Nella maggior parte dei casi si tratta di un servizio in grado di rilevare, riconoscere ed eliminare le minacce prima che possano provocare danni.

### *Flessibilità nel deployment*

Una gamma completa di opzioni per il deployment che comprenda software, appliance e servizi on-demand permette all'azienda di scegliere la soluzione più adatta alle proprie sfide ed esigenze.

Mentre le grandi aziende necessitano spesso delle funzionalità complete e del controllo granulare sulle policy tipici di una soluzione basata su software, le imprese più piccole preferiscono generalmente la semplicità e le performance elevate di una soluzione basata su appliance.

Le soluzioni on-demand rendono la protezione Internet di classe enterprise accessibile a tutte le aziende. Le organizzazioni che gestiscono molteplici uffici o addetti remoti possono utilizzare questo tipo di soluzione per soddisfare i propri requisiti in materia di sicurezza Web ed e-mail, proteggendo tutti coloro che non operano costantemente presso la sede principale. Ciò vale anche per quelle aziende che non dispongono di un'infrastruttura atta a gestire una soluzione basata su server oppure che semplicemente preferiscono demandare in outsourcing questa funzione nell'ambito della loro strategia IT complessiva.

### *Personalizzazione e controllo*

Per gestire compiutamente ogni rischio, dal malware fino all'uso inappropriato delle risorse passando per la mancata adesione alla conformità aziendale e normativa, un'azienda necessita di controlli flessibili per definire e applicare policy personalizzate sulla base del proprio ambiente, delle esigenze business e dei potenziali pericoli. La soluzione deve consentire la definizione di regole esclusive da applicare a utenti e gruppi in base al ruolo ricoperto all'interno dell'organizzazione e ai privilegi di accesso a Internet.

Una volta implementate tali policy, amministratori e responsabili aziendali necessitano di visibilità totale e capacità di reporting complete per gestire e monitorare l'impiego di Internet da parte del personale, verificare l'adesione alla conformità aziendale e normativa, e affinare la strategia di sicurezza e protezione in modo da adattarla a esigenze business in evoluzione.

### *Valore ottimale in rapporto alle esigenze*

Nello scegliere un provider per la protezione Internet, le aziende dovrebbero rivolgersi a un partner fidato e non semplicemente a un produttore interessato solo a concludere una vendita. Un partner fidato, forte di innumerevoli successi nel settore della protezione Internet e in possesso di una gamma completa di tecnologie best-of-breed è in grado di porre in campo l'esperienza, le risorse complete e l'innovazione costante indispensabili per rimanere al vertice della sicurezza. Operando in modo da comprendere appieno le esigenze di ciascun cliente, un simile provider si trova nella posizione adatta per fornire soluzioni orchestrate da un'unica regia in grado di soddisfare ogni esigenza presente, unitamente ai requisiti di supporto e aggiornamento successivi, garantendo nel tempo il massimo livello di efficacia.

La soluzione deve anche essere conveniente da acquistare, possedere, gestire e supportare nel lungo periodo, in modo tale che i costi della protezione non superino il budget IT dell'azienda anziché diventare l'ennesimo problema in attesa di una risposta.

### *La protezione in azione*

Tornando alle tre aziende oggetto degli esempi citati prima, risulta evidente come ognuno dei fattori su indicati giochi un ruolo chiave in una strategia efficace per la protezione Internet.

L'azienda A potrebbe personalizzare la sua soluzione per la protezione Internet in modo da adattarla alle policy e alle priorità esistenti, facendo quindi leva su efficaci capacità di reporting per esercitare il pieno controllo sui pericoli riscontrati.

- L'uso inappropriato di podcast e reti peer-to-peer viene totalmente bloccato, liberando risorse di rete preziose ed eliminando ogni rischio di violazione dei copyright.
- Ogni e-mail viene controllata alla ricerca di parole chiave e contenuti specifici relativi alla proprietà intellettuale dell'azienda, evitando qualunque fuga di informazioni riservate.
- L'Instant Messaging e la navigazione sul Web vengono posti sotto completo controllo, facilitando l'adesione alla conformità aziendale e normativa.
- I siti Web non sicuri e non legati alla produttività vengono bloccati, così da costringere chi gioca d'azzardo a farlo fuori dall'ambiente di lavoro e senza utilizzare le risorse dell'azienda.

L'azienda B potrebbe estendere la protezione dal perimetro della rete fino ai desktop e oltre. Indipendentemente dal modo e dal luogo in cui gli utenti remoti si collegano alla rete - abitazione, albergo, hot-spot di un luogo pubblico, rete di un cliente o ISP wireless - qualunque minaccia per i PC portatili viene bloccata prima che possa penetrare nell'ambiente aziendale. Anche i dispositivi storage rimovibili beneficiano della medesima protezione.

L'azienda C, infine, può optare per un servizio on-demand al posto di un'installazione hardware o software, beneficiando di una protezione completa senza uscire dai budget. L'azienda conserva i livelli di controllo e gestione tipici di una soluzione basata su rete o su gateway, e contemporaneamente può sfruttare i tempi rapidi di implementazione e lo scarso appesantimento che derivano dal supporto e dalle risorse di un leader specializzato.

#### *Innalzare il livello della protezione tramite le nuove soluzioni SurfControl*

Leader da lungo tempo nella sicurezza Internet, SurfControl ha innalzato il livello della protezione attraverso lo sviluppo di soluzioni progettate per fornire livelli ottimali di sicurezza, controllo e valore nell'ambito di partnership personalizzate con ciascun cliente.

#### *Protezione accresciuta*

Le soluzioni e le tecnologie best-in-class per la protezione Internet sviluppate da SurfControl hanno stabilito da tempo lo standard di riferimento per la prevenzione delle minacce. Studiate per proteggere qualunque ambiente di rete, le soluzioni SurfControl possono essere implementate sulla base delle esigenze specifiche del cliente - presso qualsiasi punto vulnerabile e in ogni formato - in modo da fornire una protezione completa a livello Web, e-mail e client. Una tecnologia euristica real-time avanzata è integrata da team esperti in analisi delle minacce dislocati in tutto il mondo, impegnati ininterrottamente per identificare e contrastare qualunque pericolo emergente compresa ogni tipologia di malware, attacco "del giorno zero" e minaccia diversificata.

#### *Superiore controllo*

SurfControl ha migliorato ulteriormente i propri tool personalizzabili per la gestione, il monitoraggio e il reporting in modo da assicurare ai clienti una superiore visibilità e aiutarli a definire, amministrare, controllare e applicare in maniera più efficace le loro policy. In particolare, le aziende beneficiano di:

- Superiore conoscenza operativa e applicazione rigorosa delle policy - Solidi quanto intuitivi tool assicurano piena visibilità sui comportamenti del personale, sull'impiego delle risorse e sull'esposizione alle potenziali minacce, aiutando le aziende ad affinare le loro policy di sicurezza e ad accertarne la scrupolosa applicazione. Il monitoraggio integrale dei contenuti permette di ridurre l'esposizione ai rischi di natura legale e normativa associati all'uso inappropriato delle risorse e alla violazione delle policy.
- Protezione delle risorse - La fuga di proprietà intellettuali può rivelarsi dannosa come ogni altra minaccia tecnologica. SurfControl pone le aziende nella condizione di monitorare tutto il traffico e-mail inbound, outbound e interno, e di proteggere i desktop dai dispositivi storage rimovibili impedendo qualunque fuga di informazione proprietaria, confidenziale o comunque sensibile.

#### *Partnership e valore credibili*

Le aziende debbono potersi fidare di chi fornisce una soluzione per la protezione. Dal 1997 SurfControl ha fornito soluzioni per la protezione Internet innovative ed efficaci a migliaia di aziende e a milioni di utenti in ogni settore e in ogni angolo del mondo. La presenza globale, la solidità finanziaria, la leadership tecnologica e l'impegno incessante da parte della società verso la protezione Internet ed e-mail arricchiscono ogni soluzione SurfControl di un'expertise e una competenza che non hanno eguali.

Prestando ascolto alle richieste di ogni cliente e comprendendone appieno le esigenze, SurfControl è in grado di proporre soluzioni mirate che forniscono una protezione conveniente sotto ogni punto di vista, dal costo di acquisizione fino alla manutenzione ed ai requisiti tecnici.

Per maggiori informazioni sul modo in cui SurfControl è in grado di innalzare il livello di protezione anche della tua azienda puoi visitare l'indirizzo: [www.surfcontrol.com](http://www.surfcontrol.com).