



Il Filtering che incrementa concretamente la produttività



INTERNET: DA STRUMENTO PRODUTTIVO A MINACCIA PER LA RETE AZIENDALE

L'evoluzione subita da Internet lo ha trasformato in una cruciale fonte di informazioni apparentemente inesauribile. Per contro però questo strumento viene spesso utilizzato per ricerche non correlate all'attività professionale. L'abuso di questo potente mezzo da parte degli impiegati può avere per qualunque azienda gravi conseguenze in termini di spreco di risorse (tempo / denaro) ed eventuale concorso in responsabilità legali.

A causa della proliferazione di contenuti inappropriati, sessualmente espliciti o potenzialmente pericolosi, l'internet si sta trasformando sempre più velocemente in una minaccia per le reti aziendali. Le aziende, che da un lato consentono ai propri impiegati di accedere dalla propria rete ad internet o, viceversa, di avvalersi delle risorse o dei servizi messi a disposizione sulla rete aziendale attraverso collegamenti remoti, dall'altro devono applicare le normative relative alla prevenzione di comportamenti inappropriati, non etici o illeciti da parte dei propri impiegati. Tale responsabilità non è quindi esclusivamente dettata dagli interessi aziendali ma anche da vincoli legali ed etici concernenti la protezione della privacy dei propri clienti e dei partner commerciali. Per molte aziende è ormai decisamente necessario garantire che l'impiego di internet in un contesto aziendale sia legato esclusivamente all'attività professionale. Basti pensare che una singola ora di navigazione di natura privata costa ad un'azienda con 100 impiegati circa € 400.000 all'anno! Un efficace filtraggio delle URL deve essere quindi una componente essenziale per garantire la sicurezza della rete aziendale.

IL BROWSER E' ESPOSTO

Agli albori di internet la maggiore sfida per i sistemi di filtraggio era la creazione banche dati di URL tanto complete da rendere improbabile che uno studente o un impiegato potessero accedere via web a contenuti illeciti. Purtroppo però il crescente impiego di internet è foriero di nuove minacce a livello di contenuti, minacce che rappresentano sia nuove opportunità sia nuove sfide per qualunque sistema di filtraggio web.

Di fronte al perfezionamento delle tecnologie dei firewall e dei sistemi antivirus per i PC, gli hacker ed i criminali informatici si sono resi conto che l'unico punto d'accesso ai dati critici è il browser. Le minacce provenienti dal web sono uno dei pericoli informatici con il tasso di crescita più elevato perché la maggior parte delle aziende lasciano aperte le porte 80 e 443 sui propri firewall. Di conseguenza il browser è diventato uno dei punti deboli della sicurezza perimetrale. Secondo Symantec infatti, il 40% degli attacchi informatici sono diretti al browser.

Anche la tipologia di queste nuove minacce alla sicurezza informatica è cambiata. Mentre i virus tradizionali possono essere individuati tramite algoritmi e/o l'abbinamento di schemi tipici, lo spyware si scarica in genere direttamente da un server. Per aggirare la scansione tradizionale dei codici, i programmatori di spyware ricompilano automaticamente questi programmi aggiungendo linee casuali per camuffare i codici reali. Di conseguenza ogni singolo codice binario di spyware scaricato può essere unico nel suo genere, rendendo assolutamente inefficace la scansione tradizionale dei malware.



AREA CULTURALE

IP Security

FILTRAGGIO delle URL

Per contro il filtraggio delle URL (indirizzi web) è un sistema relativamente efficace per bloccare spyware noti e non noti. Mentre infatti i codici binari dello spyware subiscono frequenti modifiche, gli indirizzi dei siti che installano tali programmi sono meno volubili. Sebbene da un lato questa situazione offra nuove opportunità ai sistemi di filtraggio web, dall'altro può avere notevoli ripercussioni, qualora i filtri URL siano incompleti o la valutazione dell'affidabilità dei siti sia inaccurata. La copertura e l'accuratezza dei filtri URL assumono quindi un'importanza sempre più vitale per definirne l'efficacia.

Allo stesso tempo però l'efficacia dei filtri URL tradizionali contro i contenuti illeciti viene erosa lentamente da nuove dinamiche: con l'affermazione sul mercato della prima generazione di tecnologie per il filtraggio dei contenuti web sono diventati altrettanto noti i sistemi per aggirarle. Grazie alle informazioni reperite tramite il "social networking" qualunque operatore è in grado di ingannare la prima generazione di filtri URL statici. Siti multilingua, siti d'archivi o per la ricerca di immagini e proxy personali vengono di frequente menzionati nei forum online come strumenti antifiltraggio.

La "copertura" fornita dalla banca dati e l'accuratezza della classificazione dei siti sono fattori decisivi per garantire politiche di accesso ai contenuti web appropriate e sicure. La carenza di uno dei due elementi renderebbe inutile una qualunque policy di filtro e renderebbe vulnerabili gli utenti. Va da sé che l'utilità dei sistemi di filtraggio web risiede anche nella loro abilità di essere "a prova di futuro", ossia di garantire una copertura ottimale sia dei siti noti sia di quelli a venire. L'architettura dovrà altresì fornire strumenti che riflettano accuratamente la complessità insita nelle pagine web odierne. Strutture di classificazione eccessivamente semplificate vengono velocemente sopraffatte da milioni di siti unici e spesso multidisciplinari. Questi sono solo alcuni degli elementi da considerare per poter offrire un alto livello di protezione via banca dati ed una valutazione accurata dell'affidabilità dei siti.

I criteri di selezione di sistemi di filtraggio web più rilevanti sono quindi l'efficacia della protezione fornita e la rilevanza delle categorie di filtro offerte. L'adattabilità della banca dati URL alle esigenze dell'utente a cui si rivolge è infatti più utile che una banca dati sovradimensionata. La sfida quotidiana dei moderni sistemi di filtraggio web è costituita dal fatto che ogni giorno appaiono e scompaiono migliaia di siti. Ne consegue che è più utile e aggiornare la banca dati di frequente che aggiungere nuovi siti ad una banca dati che ormai è diventata obsoleta.

LA SOLUZIONE DI NETASQ

NETASQ offre ai propri clienti soluzioni di filtraggio web che si adattano alle legittime esigenze degli utenti. Una banca dati URL viene integrata all'interno dei dispositivi di prevenzione contro le intrusioni ed il suo formato viene adeguato a necessità specifiche, includendo comunque una verifica degli indirizzi web con una banca dati che contiene diversi milioni di registrazioni.

Quindi la banca dati "personalizzata" viene fornita in un formato pre-compilato e proprietario che consente l'impiego parallelo di algoritmi di elaborazione già presenti in ASQ per le firme contestuali.

Grazie alla scelta di natura tecnologica operata da NETASQ, gli utenti possono navigare indisturbati anche qualora la funzione di filtro web sia attivata sui dispositivi UTM. Infatti la latenza dovuta all'attivazione di questa caratteristica sulle appliances di NETASQ è inferiore ad un millisecondo, meno che sbattere le palpebre.

I clienti possono avvalersi di due soluzioni di alta qualità:

1. La banca dati URL di NETASQ, ricompilata sulla base delle migliori banche dati open source esistenti sul mercato
2. Un elenco proprietario curato dal reparto di ricerca e sviluppo di NETASQ. Questo elenco viene fornito gratuitamente con tutti i dispositivi di NETASQ ai clienti che dispongono di un contratto di manutenzione di base o "privilege" valido.



AREA CULTURALE

IP Security

UNA STIMA DEL RITORNO SULL'INVESTIMENTO

Per poter facilmente illustrare il valore di sistemi di controllo dell'accesso ad internet è necessario stimare la perdita di produttività legata ad una consultazione di contenuti web non attinente all'attività professionale. In particolare ci baseremo sugli studi pubblicati da importanti enti di ricerca che attestano la quota dedicata alla navigazione di natura privata intorno al 30% - 40% della giornata lavorativa degli impiegati. Un esempio cauto è quello di un'azienda con 25 impiegati che utilizzano regolarmente il PC. Supponendo che ogni impiegato perda 60 minuti al giorno per la navigazione non inerente all'attività lavorativa e che ogni impiegato guadagni una media di 20.00 € lordi all'ora, il costo di tale attività per l'azienda supererebbe i 100.000 € annui!

Stipendio orario	Tempo perso in ore	Giorni di lavoro per anno	Numero di impiegati	Perdite annuali per l'azienda
20 €	1	220	25	110,000 €
20 €	1	220	100	440,000 €
20 €	1	220	500	2,200,000 €
20 €	1	220	1000	4,400,000 €
20 €	1	220	1500	6,600,000 €

WEB FILTERING AVANZATO (PARTNERSHIP con OPTENET)

Onde garantire ai propri clienti l'accesso alla migliore tecnologia di filtraggio web sul mercato NETASQ si è unita ad OPTENET ed offre una banca dati opzionale del leader europeo della sicurezza web. La banca dati avanzata di OPTENET beneficia delle prestazioni dell'architettura ASQ, cuore dei dispositivi UTM di NETASQ. OPTENET dispone di milioni di referenze in tutta Europa che attestano la qualità delle sue soluzioni. È quindi un partner affidabile per NETASQ e per i suoi clienti.

I sistemi di NETASQ con l'opzione Optenet proteggono più di 5 milioni di utenti ed offrono:

Banca dati URL plurilingue:

Sviluppata per l'operatività in 7 lingue — Spagnolo, Inglese, Francese, Portoghese, Tedesco, Italiano e Olandese.

Facilità d'impiego:

Latenza inferiore al millisecondo.

Servizio di sblocco online a livello mondiale:

I filtri web di OPTENET sono dotati di un servizio di sblocco dei siti per correggere eventuali errori dovuti ad un blocco eccessivo dell'accesso ai siti. Le URL bloccate vengono revisionate manualmente e sbloccate entro 10 minuti! Tale compito non è mai a carico dell'amministratore di sistema.

Reportistica avanzata:

Uno dei sistemi di reportistica e classificazione di URL disponibili sul mercato. È possibile generare un'ampia gamma di report per coprire diversi tipi di analisi quali le informazioni sul consumo di banda, la produttività degli utenti, gruppi di utenti ecc.

Funzioni	Portata
Categorie disponibili	>50
Nuove categorie	Si
Profili di filtro	Illimitati
Profili per utente / indirizzo IP	Illimitati
Pianificazione in base ai profili di filtro	Si
Elenchi personali	Liste bianche e nere
Rapporti	Si: report dettagliati ed altamente personalizzabili
Aggiornamento	Continuo, automatico ed incrementale
Supporto LDAP	Si