

Messaggistica istantanea, VoIP, P2P e giochi sul luogo di lavoro: come riprenderne il controllo

L'installazione e l'utilizzo, da parte dei dipendenti, di applicazioni non autorizzate quali messaggistica istantanea, VoIP, giochi e applicazioni per la condivisione di file peer-to-peer è fonte di forti preoccupazioni per le aziende. Questo documento spiega l'importanza di controllare tali applicazioni, tratta i diversi approcci possibili e sottolinea come l'integrazione di questa funzione nella protezione dal malware sia la soluzione più semplice e più efficiente economicamente.

Messaggistica istantanea, VoIP, P2P e giochi sul luogo di lavoro: come riprenderne il controllo

I reparti IT hanno da tempo compreso la necessità di impedire che virus, spyware e altre applicazioni o attività malevole compromettano la sicurezza e interrompano la continuità dell'azienda.

Ora il rapido emergere del Web 2.0 sta cominciando a ridefinire il modo in cui gli individui interagiscono con Internet, mentre le relative tecnologie pongono una serie di nuove minacce. Gli utenti del web più scaltri, e che possiedono diritti di amministrazione locali sui rispettivi computer di lavoro, stanno scaricando applicazioni come quelle di messaggistica istantanea (IM), condivisione file peer-to-peer (P2P) e Voice over Internet Protocol (VoIP) per poter comunicare, condividere file e lavorare con altre persone online, sia per attività ufficiali che non ufficiali.

Nel settembre 2006, in un sondaggio online Sophos ha chiesto agli amministratori IT per quali applicazioni vorrebbero impedire l'accesso e l'utilizzo ai rispettivi utenti.¹ I risultati, illustrati nella Figura 1, rivelano chiaramente il desiderio di esercitare maggiore controllo e di impedire agli utenti l'installazione e l'utilizzo di applicazioni indesiderate. Per esempio, l'86,1 per cento degli interpellati ha risposto di volere l'opportunità di bloccare le applicazioni VoIP che consentono di telefonare tramite Internet, mentre il 62,8 per cento si è spinto oltre indicando il blocco come indispensabile.

La portata del problema è percepibile anche da un recente rapporto, secondo il quale il 50 per cento degli utenti sui luoghi di lavoro scarica tool IM gratuiti da Internet, con il 26 per cento dei datori di lavoro ignari di tali azioni.²

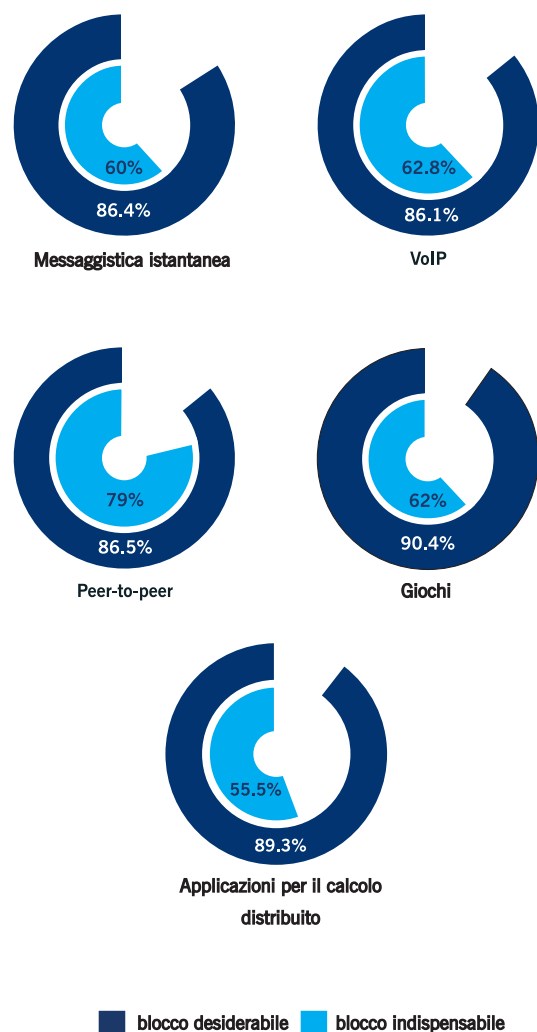


Figura 1: per gli amministratori IT il controllo delle applicazioni è fondamentale

La sfida del software non autorizzato

Le attuali difese delle aziende non proteggono in modo adeguato contro la nuova serie di minacce poste da questo comportamento degli utenti. Le difficoltà presentate da alcune applicazioni software legittime sollevano particolari problemi che vanno ben oltre la "semplice" protezione contro il malware. Per aumentare la sicurezza e la produttività, i reparti IT devono porre un limite ai diritti di accesso per le applicazioni non essenziali e controllare l'utilizzo di quelle autorizzate per le attività dell'azienda. In pratica, si tratta di una sfida non indifferente.

“

“4.1 L'utente concorda che il Software Skype può utilizzare il processore e la larghezza di banda del computer (o altro dispositivo del caso) al solo scopo di agevolare le comunicazioni tra utenti del Software Skype.”³

”

Una parte fondamentale di essa consiste nel fatto che molti utenti devono essere amministratori locali, ricevendo i necessari privilegi, per poter scaricare le applicazioni necessarie a svolgere il proprio lavoro, come ad esempio gli aggiornamenti al software Adobe Acrobat. Questo implica che possono anche scaricare, installare e utilizzare diversi altri software. Ciò rende la vita di un amministratore IT particolarmente difficile: il software malevolo viene bloccato dai programmi antivirus, ma le applicazioni come quelle di messaggistica non sono in alcun modo malevole. Non vengono installate automaticamente di nascosto e non tentano di autoreplicarsi o di sottrarre informazioni riservate.

Nondimeno, l'installazione e l'uso non autorizzati e non controllati di tale software da parte dei dipendenti sui computer aziendali presenta una minaccia reale e crescente da quattro punti di vista:

- violazioni della legge, delle normative e della sicurezza
- maggior lavoro di assistenza per l'IT
- sovraccarichi per rete e sistema
- problemi di produttività dei dipendenti.

Violazioni della legge, delle normative e della sicurezza

Leggi come quella sulla tutela dei dati personali impongono ulteriori obblighi agli amministratori IT per mantenere e proteggere l'integrità dei dati memorizzati nelle rispettive reti. Quindi l'installazione di applicazioni non autorizzate può comportare un significativo rischio dal punto di vista legale oltre che per la sicurezza dell'azienda.

Per esempio, l'utilizzo incontrollato della messaggistica istantanea rappresenta un grave rischio legale e per la sicurezza in quanto il contenuto delle chat IM spesso include allegati, barzellette, pettegolezzi e commenti denigratori, informazioni riservate su azienda, dipendenti e clienti, oltre a riferimenti di natura sessuale.

In aggiunta ai rischi legali, la messaggistica mette a repentaglio la sicurezza, a causa della crescita esponenziale degli attacchi del malware basato sull'IM. Allo stesso modo le applicazioni P2P, in aumento, sono note come vettori di codice malevolo (per l'esecuzione di comandi in remoto o l'esplorazione remota del file system) o di virus che si originano dai file.

Maggior lavoro di assistenza per l'IT

Se non adeguatamente testate e installate dal reparto IT dell'azienda, le applicazioni non controllate possono causare problemi di stabilità o di prestazioni ai computer aziendali. Oltre a essere un ulteriore e inutile grattacapo per gli amministratori IT, la risoluzione di questi problemi rappresenta anche uno spreco significativo della risorsa più preziosa a disposizione degli IT: il tempo.

Sovraccarichi per rete e sistema

La larghezza di banda della rete aziendale e la capacità di elaborazione consumati dalle applicazioni non autorizzate possono avere un diretto impatto negativo sulle risorse e la disponibilità della rete. Per esempio, i progetti di calcolo distribuito utilizzano la capacità “d'avanzo” di milioni di computer per contribuire alla creazione di modelli o di scenari simulati, ad es. per il cambiamento climatico. Anche i VoIP utilizzano tale capacità inutilizzata. In un contesto aziendale, tale attività può rallentare la rete, sovraccaricando inutilmente il reparto IT.

Problemi di produttività dei dipendenti.

Il VoIP e l'IM in particolare possono comportare vantaggi in termini di business e produttività. Tuttavia possono distrarre se utilizzati in modo non appropriato e, nella maggior parte dei casi, questi tipi di applicazione non sono indispensabili agli utenti per gli scopi dell'azienda. Un esempio più estremo di produttività ridotta è dato dall'uso di videogiochi o dalla condivisione di musica e file tramite il software peer-to-peer.

“*Quando ho scritto il Solitario per Microsoft, ho generato un mostro di improduttività. Se avessi un centesimo per ogni ora che va sprecata in ufficio con il Solitario, potrei assumere Bill Gates come portabastoni quando gioco a golf.*”⁴

Strategie di controllo delle applicazioni

Alla luce di questa ampia gamma di minacce che le applicazioni legittime ma non autorizzate possono (seppur inaspettatamente) causare, gli amministratori IT hanno tentato diverse soluzioni. Se ciascuna strategia ha qualche merito, comporta anche degli svantaggi.

Blocco dei computer

Uno dei modi più semplici per fermare l'installazione di applicazioni non autorizzate è quello di bloccare tutti i computer assegnando i diritti di amministratore solo in pochi casi. Comunque, questo è proprio il modo in cui in passato il controllo delle applicazioni è fallito.

Alcuni reparti – in particolare IT e supporto tecnico – hanno ovviamente bisogno dei diritti di amministrazione. Sarebbe ovvio consentire a tali gruppi tecnici di installare applicazioni e impedire agli altri di fare altrettanto. Purtroppo, nella pratica ciò non è così facile come sembra.

Per molte organizzazioni è costoso bloccare i computer di alcuni o di tutti gli utenti non tecnici. La scarsa flessibilità di tale strategia implica la creazione di innumerevoli criteri. Per esempio, molte semplici funzioni di Windows, quali l'aggiunta del driver di una stampante che non era incluso in Windows, la modifica del fuso orario e la regolazione delle impostazioni di risparmio energetico, non sono possibili per gli account utente standard e pertanto richiedono il continuo cambiamento dei diritti assegnati. Il maggior impegno del personale e i più lunghi tempi di risposta legati alla gestione centralizzata di ogni modifica a un computer rappresentano un costo significativo per l'impresa.

Installazione di prodotti appositi per il controllo delle applicazioni

Sul mercato esistono dei prodotti specificamente progettati per decidere quali applicazioni possono o non possono essere eseguite su un computer. Tali prodotti convalidano un'applicazione per l'utilizzo confrontandola con vasti database di applicazioni consentite e bloccate.

Per gli amministratori IT, costituiscono un ulteriore programma da valutare, acquistare, installare e gestire. La gestione di queste soluzioni non è un compito da poco ed è spesso difficile a causa delle dimensioni e della complessità delle liste di consenso e di blocco. Inoltre, se i prodotti per il controllo delle applicazioni sono efficaci nel bloccarne l'esecuzione, hanno difficoltà nell'arrestarne l'installazione iniziale.

“...se i prodotti per il controllo delle applicazioni sono eccezionali nel bloccarne l'esecuzione, hanno difficoltà nell'arrestarne l'installazione iniziale.⁵”

Infine, i prodotti specifici per il controllo delle applicazioni non forniscono protezione completa contro il malware e le imprese devono investire di nuovo in altri prodotti per la sicurezza, per tutelarsi contro virus, spyware e altre minacce.

Attuazione di regole firewall e di un sistema HIPS aziendali

Firewall e HIPS (Host-based Intrusion Prevention Systems, sistemi di prevenzione delle intrusioni basati su host) sono generalmente finalizzati a bloccare il traffico di rete potenzialmente malevolo e i tentativi di esecuzione del codice, piuttosto che a controllare quali applicazioni gli utenti possono o non possono installare e/o utilizzare. Possono essere utili nel limitare l'uso di applicazioni non autorizzate grazie al controllo dell'accesso alla rete o a Internet, per esempio cercando e bloccando il traffico VoIP, ma sono ben lungi dall'essere una soluzione adeguata al problema.

Maggior rendimento della propria soluzione antimalware

La maggior parte delle soluzioni antivirus e antispyware non offrono la funzione di controllo delle applicazioni. Comunque, un'azienda potrà ottenere di più dall'investimento nella protezione contro il malware, se la stessa infrastruttura di scansione e gestione viene utilizzata dal prodotto per intercettare e gestire l'utilizzo delle applicazioni software legittime.

Un solo client da distribuire

L'antivirus costituisce un investimento necessario che gli amministratori IT non possono fare a meno di acquistare, installare e gestire. Con una nuova funzione incorporata in questo client obbligatorio, i reparti IT possono a un tempo incrementare la resa dell'investimento e risparmiare risorse di sistema e di gestione. La distribuzione di un unico client che include antivirus, antispyware, antiadware e controllo delle applicazioni non autorizzate comporta il risparmio di tempo, denaro e risorse di sistema, oltre ad aumentare la sicurezza.

Controllo e impostazioni dei criteri più semplici

Se le funzioni antimalware e di controllo applicazioni sono combinate in un singolo prodotto, gli amministratori possono mettere in pratica le politiche aziendali di rimozione delle applicazioni non autorizzate tramite la funzione di gestione centralizzata fornita dal componente antimalware. L'affiancamento, ai criteri antivirus, di criteri di controllo delle applicazioni, migliora l'efficienza della gestione e dà l'opportunità di distinguere le esigenze dei diversi gruppi di computer. Per esempio, il VoIP potrebbe essere bloccato per i computer dell'ufficio ma autorizzato per i computer remoti, e/o il download e l'uso di software IM non autorizzato o di giochi sarebbe controllabile.

Eliminazione dei costi di amministrazione

L'utilizzo degli stessi meccanismi di gestione e aggiornamento per il controllo delle applicazioni e per il software antivirus, comporta ovvi vantaggi in termini di infrastruttura e di costi. Comunque, il successo complessivo della combinazione di tali funzioni, per quanto riguarda l'efficienza, dipende dal modo concreto in cui le applicazioni vengono rilevate.

Un approccio scelto da alcuni produttori richiede agli amministratori la creazione di firme specifiche per le applicazioni tramite l'utilizzo di nomi file che compaiono nelle applicazioni stesse. Questo metodo è però dispendioso in termini di tempo e di risorse IT. Scaricare il fardello dell'aggiornamento sull'amministratore ed è anche inaffidabile in quanto gli utenti possono semplicemente modificare il nome del file per evitare il rilevamento dell'applicazione.

In un approccio alternativo (quello scelto da Sophos), il produttore crea e aggiorna le firme di rilevamento con lo stesso metodo utilizzato per l'aggiornamento automatico del rilevamento del malware.

Semplificando amministrazione, aggiornamento e manutenzione del rilevamento, questo secondo metodo rappresenta un significativo avanzamento rispetto alle soluzioni che richiedono agli amministratori la manutenzione delle liste di consenso e di blocco o la creazione di firme tramite file o nomi file.

Minore lavoro di assistenza

Utilizzando il rilevamento basato sulla firma, che non solo arresta l'esecuzione delle applicazioni, ma ne blocca anche il download e l'installazione, un'organizzazione riduce il tempo impiegato dal supporto tecnico per individuare i computer destabilizzati dall'installazione di applicazioni non autorizzate.

Conclusioni

I problemi posti dall'installazione di applicazioni non autorizzate sui computer aziendali sono significativi. Se da un lato esistono varie soluzioni per aiutare gli amministratori IT a gestire il problema, un gran numero di esse richiede investimenti ulteriori che, per molte organizzazioni possono essere costosi, inefficienti e difficili da mantenere. Una soluzione migliore è quella che integra completamente il blocco delle applicazioni non autorizzate nella rilevazione antimalware e nell'infrastruttura di gestione esistenti. Ciò fornisce agli amministratori IT – per i quali la protezione antimalware è indispensabile – una soluzione semplice che rimuove dall'equazione i costi monetari e gestionali.

La soluzione Sophos

Application Control è una funzione opzionale di Sophos Anti-Virus versione 6 e fa parte dell'impegno di Sophos verso un sistema di sicurezza e controllo completo che utilizza un'unica console di gestione e un client universale per tutti gli aspetti della gestione operativa dal desktop, non solo per la sicurezza.

Per maggiori informazioni sui prodotti Sophos e su come valutarli, visitate www.sophos.it

Fonti

- 1 Sondaggio web Sophos
- 2 2006 Workplace E-Mail, Instant Messaging & Blog Survey from American Management Association (AMA) and The ePolicy Institute.
- 3 Contratto di Licenza per Utente Finale Skype, Articolo 4 Uso del computer dell'utente
- 4 Wes Cherry, autore del Solitario di Microsoft Windows, parlando con Sophos
- 5 Windows Application Control Solutions Provide an Alternative for Desktop Lockdown, Gartner Inc. marzo 2006

Informazioni su Sophos

Sophos è società leader a livello mondiale nelle soluzioni per la protezione integrata dalle minacce informatiche, concepite su misura per le aziende, il settore education e la Pubblica Amministrazione. Grazie all'esperienza ventennale e alla profonda conoscenza di virus, spyware e spam, i SophosLabs proteggono persino le reti più complesse da minacce note e sconosciute. I prodotti Sophos, affidabili e facili da utilizzare, proteggono oltre 35 milioni di utenti in più di 150 Paesi contro virus, spyware, intrusioni, applicazioni indesiderate, phishing, spam e violazioni delle policy di posta. Prestigio internazionale, solidità finanziaria e un portafoglio clienti in continua espansione sono la chiave del successo di Sophos. Tempi di reazione brevissimi e supporto tecnico 24x7, interamente dedicato al mondo business, garantiscono a Sophos un invidiabile livello di soddisfazione dei clienti.

Boston, USA • Magonza, Germania • Milano, Italia • Oxford, UK • Parigi, Francia
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Giappone

© Copyright 2007. Sophos Plc.

*Tutti i marchi e i marchi registrati sono proprietà dei rispettivi titolari.
Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, senza previa autorizzazione scritta del titolare dei diritti d'autore.*

SOPHOS
WWW.SOPHOS.COM