

## **Proteggere la rete dalle minacce di posta elettronica**

Il bisogno di una sicurezza della posta elettronica completa e basata sul server

Questa white paper spiega perché un solo software antivirus non sia sufficiente a proteggere l'azienda da attacchi presenti e futuri di virus e minacce email. Con un'analisi dei diversi tipi di attacchi e problemi di posta elettronica che minacciano oggi le aziende, questo documento illustra la necessità di una soluzione efficace per la sicurezza delle email basata sul server al fine di salvaguardare la propria rete.

---

## Introduzione

La presente white paper spiega perché un solo software antivirus non sia sufficiente a proteggere l'azienda da attacchi presenti e futuri di virus di computer. Con un'analisi dei diversi tipi di minacce email e di metodi per attaccare la posta elettronica, questo documento illustra la necessità di un efficace gateway per il controllo del contenuto basato sul server, al fine di proteggere la propria attività da virus di posta elettronica, attacchi e fughe di informazioni.

Introduzione.....	2
La minaccia costituita da virus di email e Trojan.....	2
La minaccia costituita dalle fughe di informazioni.....	3
La minaccia costituita da email dal contenuto pericoloso od offensivo.....	3
Metodi utilizzati per attaccare il sistema di posta elettronica.....	3
La sconvolgente facilità con cui è oggi possibile creare un virus.....	5
Perché un software antivirus o un firewall non sono sufficienti.....	5
La soluzione: un approccio proattivo.....	6
Informazioni su GFI MailSecurity for Exchange/SMTP.....	6
Informazioni su GFI.....	7

---

## La minaccia costituita da virus di email e Trojan

L'esteso utilizzo della posta elettronica ha fornito ad hacker e cracker un modo facile per diffondere contenuti dannosi alle reti interne. Gli hacker possono con facilità aggirare la protezione offerta da un firewall attraverso la tecnica del *tunnelling* del protocollo email, poiché esso non analizza il contenuto delle email.

Nel gennaio 2004, la CNN ha riportato che il virus MyDoom è costato alle aziende circa 250 milioni di dollari USA in termini di mancata produttività e spese di assistenza tecnica, mentre NetworkWorld (nel settembre 2003) ha citato studi che hanno collocato il costo della lotta a Blaster, SoBig.F, Wechia ed altri virus di posta elettronica, a 3,5 miliardi di dollari USA per le sole aziende statunitensi.

La posta elettronica è inoltre utilizzata per installare Trojan, mirati in modo particolare alle singole organizzazioni per ottenere informazioni confidenziali o prendere il controllo dei loro server. Descritti come "virus che danno istruzioni al computer" o "virus spia" da esperti di sicurezza informatica, essi possono costituire potenti strumenti di spionaggio industriale. Un esempio è stato l'attacco alla rete di Microsoft avvenuto nell'ottobre 2000, descritto da un portavoce dell'azienda come "un atto di spionaggio industriale puro e semplice". Secondo quanto riportato, la rete di Microsoft è stata violata mediante un virus Trojan backdoor inviato via email ad utente della rete, con l'intento di arrecare pregiudizio.

---

## **La minaccia costituita dalle fughe di informazioni**

Spesso le organizzazioni trascurano di riconoscere l'esistenza di un forte rischio di furto di dati fondamentali proveniente dall'interno dell'azienda. Diversi studi hanno dimostrato che i dipendenti utilizzano la posta elettronica per diffondere informazioni aziendali confidenziali. Che le ragioni risiedano nel loro essere scontenti o nel volersi vendicare, oppure perché non riescono a comprendere pienamente l'effetto negativo di tale prassi, i dipendenti utilizzano la posta elettronica per condividere dati sensibili ufficialmente destinati a restare all'interno.

Come ha dimostrato nel 2003 l'inchiesta Hutton nel Regno Unito, si è scoperto che funzionari governativi e dirigenti della BBC hanno utilizzato la posta elettronica per rivelare informazioni confidenziali. Nel marzo 1999, un articolo apparso su PC Week faceva riferimento ad uno studio in cui, su 800 lavoratori intervistati, una percentuale compresa tra il 21 e il 31% ha ammesso di inviare informazioni confidenziali, come dati finanziari o su prodotti, a destinatari esterni all'azienda.

---

## **La minaccia costituita da email dal contenuto pericoloso od offensivo**

Le email di contenuto razzista, sessista o altro materiale offensivo, inviate dal personale, possono rendere l'azienda legalmente vulnerabile. Nel settembre 2003, la ditta inglese Holden Meehan Independent Financial Advisors ha dovuto versare 10.000 sterline ad un'ex-dipendente per non averla difesa dalle molestie perpetrate via email. Com'è noto, Chevron ha dovuto versare 2,2 milioni di dollari USA a quattro dipendenti dopo che questi hanno presumibilmente ricevuto molestie sessuali via email. Ai sensi della legislazione britannica, i datori di lavoro sono ritenuti responsabili per le email scritte dai dipendenti durante il periodo di assunzione, con o senza il consenso del dipendente all'email stessa. La compagnia di assicurazioni Norwich Union ha dovuto pagare 450.000 dollari USA di accordo amichevole extragiudiziale a seguito di commenti su concorrenti inviati via email.

---

## **Metodi utilizzati per attaccare il sistema di posta elettronica**

Per capire il tipo di minacce di posta elettronica correnti, è opportuno dare un rapido sguardo ai principali metodi di attacchi via email attuali. Tra questi:

### **Allegati con contenuto maligno**

Melissa e LoveLetter sono stati tra i primi virus a far mettere in rilievo il problema degli allegati via email e della fiducia dei riceventi. Si sono infatti serviti del rapporto di fiducia esistente tra amici o colleghi. S'immagini di ricevere un allegato da un amico che vi chiede di aprirlo. Questo è appunto ciò che è successo con Melissa, AnnaKournikova, SirCam ed altri worm di email simili. Una volta in esecuzione, tali worm di solito operano inviando copie di se stessi a tutti gli

indirizzi email presenti sulla rubrica della vittima, ai mittenti di email precedenti, alle cache di pagine web della macchina locale ed altri metodi simili. Gli autori di virus pongono molta enfasi nel convincere la vittima ad eseguire l'allegato. Per questo motivo, utilizzano nomi molto promettenti per i loro allegati, come SexPic.cmd o me.pif.

Molti utenti cercano di evitare il contagio da virus di posta elettronica eseguendo solo file con estensioni sicure, come JPG o MPG. Tuttavia, alcuni virus, come il worm AnnaKournikova, utilizzano più estensioni per indurre l'utente ad eseguire il file. Il virus AnnaKournikova veniva trasmesso mediante un allegato email denominato "AnnaKournikova.jpg.vbs", che lasciava credere ai destinatari di aver ricevuto un'innocua immagine JPG della famosa tennista, anziché un Visual Basic Script che conteneva un codice infetto.

Inoltre, l'estensione Class ID (CLSID) consente agli hacker di nascondere la vera estensione de file, nascondendo così che il file "cleanfile.jpg" è in realtà uno sgradevole file HTA (applicazione HTML).

Questo metodo attualmente riesce inoltre a aggirare quelle soluzioni di filtraggio di contenuto della posta elettronica che utilizzano metodi di controllo dei file piuttosto semplici, consentendo all'hacker di raggiungere più facilmente l'utente preso di mira.

### **Email che attivano exploit noti**

Il worm Nimda colse Internet di sorpresa, aggirando molti strumenti di sicurezza per la posta elettronica e contagiando sia i singoli utenti, sia i server e le reti aziendali. La peculiarità di Nimda era data dalla sua esecuzione automatica su computer che avevano versioni vulnerabili di Internet Explorer o Outlook Express. Nimda è stato uno dei primi di una serie di virus ad aver sfruttato un difetto piuttosto che un altro per diffondersi. Le varianti del virus Bagle, emerso nel marzo 2004, per esempio, sfruttavano un vecchio difetto di Outlook nel tentativo di diffondersi senza alcun intervento dell'utente.

### **Email HTML con script incorporati**

Attualmente, tutti i client di email sono in grado di inviare e ricevere email in formato HTML.. I messaggi di posta HTML possono contenere script e *Active Content* (contenuto attivo), che consentono l'esecuzione di programmi o codici sulla macchina client. Outlook e altri prodotti utilizzano i componenti di Internet Explorer per visualizzare le email HTML, perciò "ereditano" le vulnerabilità di sicurezza riscontrate in Internet Explorer.

I virus basati su script HTML presentano l'ulteriore pericolo causato dalla loro capacità di entrare in esecuzione automatica quando l'email infetta viene aperta. Non dipendono dagli allegati, pertanto i filtri di allegati dei software antivirus si rivelano inutili nella lotta contro virus di script HTML sconosciuti.

Ad esempio, il virus BadTrans.B combina un exploit di posta elettronica con l'HTML per

propagarsi, usando HTML per eseguire automaticamente un allegato una volta ricevuta l'email.

---

## **La sconvolgente facilità con cui è oggi possibile creare un virus**

Chiunque abbia una minima conoscenza di Visual Basic è in grado di scatenare il caos semplicemente sfruttando vulnerabilità ben note di client e programmi per email comunemente usati. Una visita al sito SecurityFocus, ad esempio, rivelerà numerosi exploit per Microsoft Outlook. Uno *script kiddie* (ragazzino capace di utilizzare script) pericoloso, che voglia creare un virus, può semplicemente modificare il codice dell'exploit, il quale è disponibile pubblicamente!, per eseguire il proprio codice.

Ad esempio, suGuninski.com viene descritto un exploit per Internet Explorer e MS Access, tranquillamente applicabile ad Outlook ed Outlook Express. Il virus potrebbe contagiare tutti i file HTML e auto-inviarsi a tutti i contatti presenti sulla rubrica del ricevente. Una caratteristica chiave di questo virus quella che esso viene eseguito semplicemente quando l'utente apre l'email contenente l'HTML maligno.

---

## **Perché un software antivirus o un firewall non sono sufficienti**

Alcune organizzazioni si cullano in un falso senso di sicurezza installando un firewall. Si tratta di un asso ragionevole nella direzione della protezione della propria rete interna (intranet), ma non basta: i firewall possono impedire l'accesso alla rete da parte di utenti non autorizzati. Non controllano però il contenuto di email inviate e ricevute da coloro che sono autorizzati ad usare il sistema, ad esempio. Ciò significa che i virus di email possono superare questo livello di sicurezza.

Del resto, neanche i software antivirus proteggono da TUTTI gli attacchi e virus di posta elettronica: i produttori di antivirus non sono sempre in grado di aggiornare in tempo le loro firme nei confronti dei virus mortali diffusi in tutto il mondo via email in poche ore (come i recenti worm MyDoom, NetSky.B e Bearle). Le aziende che utilizzano un solo motore antivirus non sono necessariamente salvaguardate quando viene rilasciato un nuovo virus. Ad esempio, uno studio effettuato dal governo britannico nel 2004 ha riscontrato che, nonostante il 99% delle grosse aziende britanniche utilizzi prodotti antivirus, il 68% di loro è stato contagiato da virus nel 2003. Allo stesso modo, uno studio eseguito presso i laboratori di ricerca Hewlett-Packard di Bristol nel 2003 ha scoperto che l'approccio dell'aggiornamento delle firme per l'individuazione e rimozione dei virus era fondamentalmente difettoso, semplicemente perché i worm possono diffondersi più rapidamente della velocità di rilascio degli aggiornamenti delle firme.

---

## **La soluzione: un approccio proattivo**

Come proteggersi dunque da queste minacce di posta elettronica? È necessario un approccio proattivo, che estenda il controllo del contenuto di tutte le email in entrata e in uscita a livello del server, prima della loro distribuzione agli utenti della rete. In questo modo, prima si rimuove tutto il potenziale contenuto dannoso da un'email infetta o dubbia e solo dopo questa viene inoltrata all'utente.

Con l'installazione di un gateway antivirus e di controllo del contenuto delle email completo sul proprio server di posta, le aziende possono proteggersi dai possibili danni e dalle ore di lavoro sprecate che i virus attuali e futuri possono causare.

---

## **Informazioni su GFI MailSecurity for Exchange/SMTP**

GFI MailSecurity for Exchange/SMTP è una soluzione per il controllo del contenuto della posta elettronica, la scoperta di exploit, l'analisi delle minacce e antivirus, in grado di eliminare ogni tipo di minaccia di posta prima che sia in grado di infettare gli utenti email. Le caratteristiche principali di GFI MailSecurity comprendono: motori antivirus multipli, per garantire una percentuale d'individuazione più elevata nonché una risposta più rapida ai nuovi virus; controllo del contenuto della posta e degli allegati, per mettere in quarantena allegati e contenuti pericolosi; uno scudo contro gli exploit, per proteggere dai virus presenti e futuri basati sugli exploit; un motore per le minacce HTML, per disabilitare gli script HTML; uno Scanner per Trojan ed Eseguibili, per individuare gli eseguibili dannosi e molto altro ancora. Per saperne di più e scaricare una versione di prova, visitare il sito: <http://www.gfi-italia.com/italia/mailsecurity/>.

---

## Informazioni su GFI

GFI è una società leader nello sviluppo di software, che offre agli amministratori di rete un'unica fonte in grado di soddisfare le loro esigenze di protezione della rete, sicurezza del contenuto e messaggistica. Grazie alla tecnologia vincitrice di numerosi riconoscimenti, ad una politica tariffaria aggressiva e alla particolare attenzione rivolta alle piccole e medie aziende, GFI riesce a soddisfare le esigenze di continuità e produttività aziendali delle organizzazioni in generale. Costituita nel 1992, GFI ha uffici a Malta, Londra, Raleigh, Hong Kong, Adelaide, e Amburgo, a supporto di oltre 200.000 installazioni in tutto il mondo. GFI è orientata alla collaborazione con partner e si avvale infatti di oltre 10.000 partner in tutto il mondo. GFI è inoltre Microsoft Gold Certified Partner. Maggiori informazioni su GFI sono reperibili sul sito <http://www.gfi-italia.com>.

© 2007 GFI Software. Tutti i diritti riservati. Le informazioni contenute nel presente documento rappresentano l'attuale conoscenza della GFI, in merito agli argomenti trattati, alla data di pubblicazione. A causa di cambiamenti nelle condizioni di mercato, non deve essere considerato in alcun modo un impegno da parte di GFI, e GFI non può garantire l'esattezza delle informazioni fornite dopo la data di pubblicazione. Questa white paper deve essere considerata a puri fini informativi. GFI NON OFFRE GARANZIE, ESPLICITE O IMPLICITE, NEL PRESENTE DOCUMENTO. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor e i rispettivi loghi sono marchi registrati o marchi di GFI Software negli Stati Uniti e/o in altri paesi. Tutti i prodotti e le aziende nominate nel presente documento sono marchi registrati dei rispettivi proprietari.