

# Gestire i log secondo le disposizioni del Garante

GFI EventsManager è una soluzione di log management che consente alle imprese di conservare i dati relativi agli accessi degli Amministratori di Sistema ai sistemi da loro gestiti, secondo quanto stabilito dal Garante per la Privacy.

Il Garante per la Privacy ha stabilito che entro il 28 febbraio 2009 (prorogato al 15 dicembre 2009) tutte le aziende dovranno registrare e conservare i dati relativi agli accessi degli Amministratori di Sistema ai sistemi da loro gestiti, al fine di agevolare la *‘verifica sulla loro attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici’*. In pratica, questo significa che le imprese dovranno tracciare, mediante soluzioni di log management, gli accessi degli operatori ai sistemi in cui risiedono i dati e alle applicazioni e i dati raccolti dovranno essere conservati in maniera sicura per almeno sei mesi e dovranno essere consultabili dall'azienda e dalle autorità.

## Non vincolo ma opportunità

“In realtà la normativa – spiega **Maurizio Taglioretti**, channel sales manager per il Sud Europa – non va vissuta come un vincolo e una costrizione, ma come un’opportunità per gli amministratori di sistema. Infatti, quando si verifica un qualsiasi problema, gli amministratori devono manualmente raccogliere e verificare i log di sistema. I log degli eventi sono generati di continuo dagli utenti o in automatico da processi, per cui sono molto voluminosi. Questo e insieme il fatto che essi sono ar-

chiviati su differenti sistemi, rende le attività di raccolta, controllo e gestione lunghe e onerose. Invece, avvalendosi di soluzioni di log management tali attività possono essere velocizzate e automatizzate. *GFI EventsManager* è una soluzione compliance-ready che consente da un lato alle imprese di ottemperare alla normativa controllando i dati relativi agli accessi degli Amministratori di Sistema ai sistemi da loro gestiti e dall’altro agli stessi Amministratori di gestire i log in maniera più semplice ed efficace. Questa gestione può essere effettuata sia dall’utente finale che dai nostri partner”.

**GFI EventsManager consente alle imprese di ottemperare alla normativa controllando i dati relativi agli accessi degli Amministratori di Sistema ai sistemi da loro gestiti**

## Passare i log al setaccio

La soluzione, che è testata per raccogliere fino a sei milioni di eventi all’ora, è compatibile con diverse tipologie di eventi, come per esempio: eventi W3C Windows, Syslog, Snmp (Simple Network Management Protocol) generati da firewall, server, router, sensori e centralini. Tramite il protocollo Snmp, è possibile monitorare una vasta gamma di dispositivi hardware e creare report sullo ‘stato di salute’ di ognuno, il che migliora l’uptime della rete. GFI EventsManager consente di inviare avvisi in tempo reale qualora vengano individuati eventi critici o

intrusioni con la possibilità di attivare script o inviare notifiche tramite sms oppure e-mail. Tutti i log acquisiti vengono archiviati su un unico database SQL che può risiedere anche in remoto e protegge l'accesso mediante password criptata. Come previsto dalla normativa, le registrazioni mantengono le caratteristiche di completezza e inalterabilità e comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate. Il sistema permette inoltre di inviare/pubblicare periodicamente rapporti personalizzabili in formato PDF contenenti tutti i login-logout, manutenzioni su password, accesso, policy etc. Riassumendo, GFI EventsManager copre le seguenti aree:

- *sicurezza del sistema informativo e della rete;*
- *monitoraggio dello stato di salute del sistema;*
- *conformità a normative.*

## Anche on the cloud

Questa soluzione sarà disponibile anche in modalità SaaS, dal momento che il Garante della privacy prevede che la gestione possa essere fatta anche da



**Maurizio Taglioretti, channel sales manager per il Sud Europa di GFI Software**

terze parti. “La nostra strategia – precisa Taglioretti – punta a rendere tutte le soluzioni disponibili sia in modalità on premise che on demand (SaaS). In quest’ultimo anno abbiamo acquisito due società, Houndog (ora GFIMAX) e Katharion, che ci consentono di spostare on the cloud la nostra offerta

per la protezione della messaggistica (server fax di rete, archiviazione e gestione della posta elettronica), dei contenuti (antivirus, antispam, monitoraggio di http e ftp in tempo reale) e della rete (gestione degli eventi, scanner di porte e di vulnerabilità di rete, gestione delle patch, controllo degli end-point, monitoraggio dei server). Tra i vantaggi della sicurezza ‘sulla nuvola’ vi è la possibilità di bloccare le minacce prima che queste entrino in azienda. Si pensi per esempio alla minaccia dello spam: un antispam installato in azienda blocca lo spam una volta che questo ha ormai ‘appesantito’ il server, mentre se la soluzione è nel cloud la minaccia non arriva sul server, resta di fuori dalle mura aziendali a beneficio delle performance dei sistemi. Grazie al SaaS per le imprese si elimina la necessità di acquistare l’hardware, il software e i servizi per l’installazione e per la successiva manutenzione e, cosa non indifferente, il pagamento è relativo all’effettivo utilizzo della soluzione. Oltre che per gli utenti finali, i benefici del SaaS sono evidenti anche per i nostri rivenditori che tra l’altro con il servizio *try and buy* possono provare gratuitamente l’offerta per un mese. Tengo comunque a precisare che le soluzioni continueranno a essere disponibili anche in modalità on premise; questo perché, a differenza di alcuni nostri competitor che propendono per l’una o l’altra tipologia di offerta, siamo convinti che il futuro sarà ‘ibrido’. Il SaaS non è migliore dell’on premise – o viceversa – perché tutto dipende dalle caratteristiche e dalle esigenze del cliente”.

### Cosa si può gestire e proteggere con GFI?

GFI offre alle imprese soluzioni per la protezione della messaggistica, dei contenuti e della rete; in particolare:

- **gestione dei fax:** GFI FAXMaker rende semplici l’invio e la ricezione dei fax;
- **gestione della posta elettronica:** con GFI MailArchiver è possibile gestire la posta elettronica in linea con le esigenze di conformità;
- **protezione della posta elettronica:** GFI MailEssentials è una soluzione antispam, antiphishing e di gestione della posta elettronica per Exchange/Smtp che si avvale di due motori antispam; GFI MailDefence Suite è una soluzione antispam, antiphishing e di gestione della posta elettronica per server Exchange basata su cinque motori antivirus;
- **protezione degli end-point:** GFI EndPointSecurity consente agli amministratori di controllare attivamente l’uso di dispositivi di memoria portatili (unità Usb, palmari...) impedendo agli utenti di acquisire dati riservati e di diffondere virus e trojan nella rete;
- **monitoraggio della rete:** la rete in tempo reale: GFI NetworkServer Monitor controlla eventuali disfunzioni della rete e dei server e le ripara in maniera automatica. Gli avvisi agli amministratori possono essere inviati via posta elettronica, cercapersone o sms. GFI LANguard consente la gestione delle vulnerabilità di rete;
- **filtraggio web:** GFI WebMonitor filtra, monitora i contenuti web anche grazie a strumenti di classificazione dei siti e filtraggio web;
- **gestione dei registri degli eventi:** GFI EventsManager consente il monitoraggio, la gestione e l’archiviazione degli eventi.