

Access log “in-a-box”

Proposta tecnico-economica per ottemperare al provvedimento del 27 novembre 2008 del Garante Privacy:

"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"

Numero documento: VT-ALB-1009 rel. 1.0

Le informazioni contenute in questo documento sono riservate e confidenziali e ne è vietata la diffusione in qualunque modo eseguita. Qualora Lei non fosse la persona a cui è destinato questo documento ed indicata nelle righe qui sopra, la invitiamo ad eliminarlo e a non leggerlo, dandocene gentilmente comunicazione.

The information contained in this document and any attachments are confidential and may also be privileged. If you are not named person to read it, please notify us immediately and do not disclose the contents to another person, use it for any purpose, or store or copy the information in any medium.

La normativa

Dopo le recenti e numerose modifiche normative o "di prassi" a cui abbiamo assistito negli ultimi tempi, ecco che viene pubblicato un ulteriore provvedimento del Garante Privacy che introduce un nuovo adempimento in materia di gestione e protezione dei dati personali trattati attraverso sistemi informatici e di garanzia della sicurezza degli stessi dati e sistemi.

Il Garante Privacy, infatti, con un provvedimento del 27 novembre 2008 ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"), ha introdotto l'obbligo per gli amministratori di sistema (compresi coloro che svolgono la mansione di amministratore di rete, di data base o i manutentori), di conservare gli "access log" per almeno sei mesi in archivi immutabili e inalterabili.

Devono, cioè, essere adottati sistemi idonei alla registrazione degli accessi logici, ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema e, novità forse più importante, gli access log devono avere le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste; ciò vuol dire che le registrazioni devono avere i riferimenti temporali certi e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo (non inferiore a sei mesi). Come non pensare a processi di conservazione digitale in linea con regole tecniche previste dall'art. 71 del Codice dell'amministrazione digitale e oggi contenute nella deliberazione CNIPA n. 11/2004 e nel DPCM 13 gennaio 2004?

I titolari dovranno altresì favorire una più agevole conoscenza, nell'ambito della propria organizzazione, dell'esistenza di eventuali amministratori di sistema: è importante garantire, in questo modo, la conoscibilità dell'esistenza di tali figure e di chi svolge ruoli analoghi all'interno di tutti gli enti e le organizzazioni; viene precisato, inoltre, che gli amministratori di sistema, indipendentemente se nominati incaricati o responsabili del trattamento, devono essere sempre persone fisiche ben individuate all'interno del DPS e il loro nomi devono essere comunicati o resi conoscibili da tutti i soggetti interessati.

Per evitare spiacevoli sanzioni ogni titolare dovrà verificare che tale elencazione sia stata effettuata nell'ambito del prossimo aggiornamento annuale del DPS e, nei casi in cui il titolare non sia tenuto a redigerlo, si dovrà provvedere ad inserire il nominativo degli amministratori di sistema in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Se poi l'attività degli amministratori di sistema riguarda, anche indirettamente, servizi o sistemi che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati, in qualità di datori di lavoro, sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema all'interno delle proprie organizzazioni attraverso apposita informativa ex art. 13 d.lgs. 196/2003 (in alternativa si possono utilizzare anche strumenti di comunicazione interna quali l'intranet aziendale, ordini di servizio a circolazione interna etc.). Sono fatti salvi, in ogni caso, i casi di esclusione per legge di tale forma di pubblicità o conoscibilità.

I titolari del trattamento avranno, altresì, un obbligo di verifica annuale sull'operato degli amministratori di sistema, per controllare la rispondenza o meno alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalla normativa vigente.

In tema di esclusioni, tale provvedimento non si applica ai titolari che rientrano nel beneficio delle esenzioni privacy oggetto delle recenti misure di semplificazione, previste per le piccole e medie imprese o per i professionisti che trattano dati personali per le sole finalità amministrative e contabili.

INFORMAZIONI GENERALI

Il tema legato all'implementazione di misure di sicurezza e del rispetto della normativa sulla privacy è stato da sempre al centro dell'attenzione di quanti si trovano a gestire grandi banche dati o ad essere titolari o responsabili del trattamento o della conservazione all'interno di importanti aziende. Per quest'ultimi, infatti, sono state previste nuove cautele da rispettare nella scelta e nomina degli amministratori di sistema. L'individuazione precisa e responsabile di tali soggetti, infatti, riveste una notevole importanza, perché è una delle scelte fondamentali all'interno di un'azienda e contribuisce a incrementare la complessiva sicurezza dei trattamenti svolti. Basti pensare, infatti, che molto spesso l'amministratore di sistema è dotato di una particolare posizione a cui spetta anche la capacità di stabilire - in raccordo con il titolare e/o eventuali altri responsabili dei relativi trattamenti - chi può accedere in modo privilegiato alle risorse del sistema informativo e a tutti i dati personali aziendali (anche sensibili): per tale motivo gli amministratori di sistema devono essere scelti con particolare attenzione, poiché i rischi che possono correre le banche dati o le reti informatiche sono sempre più elevati.

Proposta

La proposta ha come obiettivo una soluzione "in-a-box" per raggiungere al **minor costo possibile** la conformità alla nuova normativa. Il termine "in-a-box" è quantomai appropriato alla soluzione trattandosi di "appliance" sul quale sono contenuti tutti i sistemi software necessari, oltre a una device esterna per il backup.

Si tratta di un sistema che raccoglie, analizza e archivia gli EventLog ed i SysLog generati da host Windows e Syslog da hosts UNIX, Router & Switches ed altri dispositivi. Attraverso la console web gli amministratori di sistema possono generare dettagliati report sugli accessi ai sistemi - per ottemperare agli obblighi delle normative - e identificare modifiche di configurazioni, errori di sistema e violazioni di sicurezza. Il sistema aiuta a monitorare le minacce interne e rispetto alle policies di sicurezza. Archivia i log per l'auditing del network e per la conformità a diverse regolamentazioni come Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), e Payment Card Industry Data Security Standards (PCI).

Ambienti supportati

Windows NT/2000/XP/Vista/2003
 Windows 2008 Server
 Linux RedHat e Debian
 UNIX
 Solaris
 HP-UX
 Switches e Routers Cisco e altri
 Windows IIS
 Web server
 FTP server
 MS SQL server

CONTENUTO DELLA PROPOSTA

Access log "in-a-box" è una soluzione completa e indipendente dall'infrastruttura presente, fatto salvo per una licenza antivirus da installare. E' licenziato per numero di sistemi da controllare e comprende:

- appliance dedicato fattore di forma 1U con manutenzione hardware NBD per 36 mesi
- licenza sistema operativo
- moduli software con tutte le funzionalità elencate con validità e manutenzione per 36 mesi
- sistema esterno per backup dei dati
- servizi di installazione e configurazione on-site

Funzionalità

Event log manager centralizzato
 Report sulla conformità
 Alerting automatico
 Trend storico
 Ananalisi sicurezza
 Host grouping
 Report eventi pre costruito
 Report personalizzabili
 Report schedulati
 Report con formati multipli

CODICE	CONTENUTO SOLUZIONE	PREZZO
AL-W1036	Appliance, moduli software per 10 nodi, installazione e configurazione	€ 6.740,00
AL-W2536	Appliance, moduli software per 25 nodi, installazione e configurazione	€ 9.490,00
AL-W5036	Appliance, moduli software per 50 nodi, installazione e configurazione	€ 11.740,00
AL-W10036	Appliance, moduli software per 100 nodi, installazione e configurazione	€ 13.740,00
AL-W20036	Appliance, moduli software per 200 nodi, installazione e configurazione	€20.390,00

Rimane escluso dalla soluzione:

- fornitura antivirus per sistema. "Access Log in-a-box" - sarà utilizzato il sistema presente nell'organizzazione
- creazione di ulteriori report oltre a quelli generati in fase di installazione e configurazione
- servizi di controllo su sistema di backup
- ogni attività legata alla gestione del sistema, ivi compreso l'aggiornamento del sistema software alla pubblicazione di nuove release