Provvedimento garante della Privacy del 27/11/2008

(abstract)

L'amministrazione dei sistemi informatici è un'attività estremamente delicata. Per il loro lavoro i System Administrator gestiscono quotidianamente dati personali, sia sensibili che non, in grande quantità. Tale attività è talmente delicata da aver richiamato l'attenzione del Garante della Privacy perché essa si svolga con le adeguate caratteristiche di sicurezza. In particolare il Garante richiede che tutte le attività di System Administration vengano opportunamente loggate e che il log sia sicuro, non modificabile.

Questo problema diventa ancora più complesso nelle realtà Enterprise. In queste realtà il numero di sistemi e sottosistemi (Basi Dati, Applicazioni, Infrastrutture di rete, DB di utenti ecc) oggetto delle attività di amministrazione è estremamente elevato ed i sistemi in questione sono spesso sistemi Legacy che non potevano essere disegnati con specifiche funzionali adatte alle necessità contemporanee.

Infine, per rendere le cose ulteriormente complesse, nelle grandi realtà spesso le attività di amministrazione dei sistemi sono appaltate a consulenti esterni, che possono variare con una certa dinamicità, e sui quali il controllo è fatalmente minore di quello che si può effettuare sul personale interno.

In dettaglio le richieste del Garante:

VALUTAZIONE DELLE CARATTERISTICHE SOGGETTIVE

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

DESIGNAZIONI INDIVIDUALI

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

ELENCO DEGLI AMMINISTRATORI DI SISTEMA

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico della sicurezza, oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

VERIFICA DELLE ATTIVITÀ

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

REGISTRAZIONE DEGLI ACCESSI

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Nella nostra visione la realizzazione di procedure informatiche per la Valutazione delle caratteristiche oggettive degli Amministratori e per la loro Designazione individuale non apporta benefici sostanziali; si tratta di attività tipicamente già svolte dall' ufficio del personale. Lo stesso può valere per gli elenchi degli amministratori di sistema; si tratta di elenchi di dimensioni limitate e che discendono direttamente dalla Designazione Individuale.

Le nostre proposta realizzative intendono, invece, concentrarsi sugli aspetti secondo noi più difficoltosi nella realizzazione della conformità: la registrazione sicura degli accessi e la verifica delle attività.