# Sicurezza, Gestione dei Sistemi ed Amministratori

Sommario:

La sicurezza dei sistemi e applicazioni ICT non è solo una questione tecnica legata al loro sviluppo e implementazione, ma un aspetto rilevante è la loro gestione soprattutto per quanto riguarda gli accessi privilegiati da parte degli amministratori di sistemi e applicazioni. Anche se molto è stato fatto negli ultimi anni, rimangono ancora aperte alcune questioni fondamentali per allineare la gestione dei rischi e della sicurezza degli accessi privilegiati ai sistemi ICT alle logiche aziendali e di business.

La sicurezza di applicazioni e sistemi IT è il risultato di una complessa interazione di molte componenti, sia tecniche che umane. Alla base ovviamente vi è il codice, ma la scrittura del codice secondo procedure “sicure” non è un evento a se, ne è sufficiente per produrre applicazioni e sistemi IT “sicuri”. Anche il significato del termine “sicuro” va contestualizzato a quali sono gli obiettivi di sicurezza che si vogliono raggiungere.

Negli ultimi anni si è posta molta attenzione a livello tecnico alla qualità intrinseca del codice, per cui problemi quali i famosi *buffer-overflow*, sono per fortuna ormai rari. Ma la sicurezza di una applicazione o di un sistema IT dipende non solo dall'assenza di errori nel codice, ma anche, o meglio soprattutto, da come questa è stata progettata e viene utilizzata. Una applicazione in cui tutti gli utenti siano amministratori ed abbiano completi privilegi su tutto, è oggi da considerarsi come una applicazione insicura.

I concetti principali e ben noti che possono portare ad una buona gestione della sicurezza sono:

- Minimi Privilegi (Least Privileges - LP)
- Separazione dei Compiti (Separation of Duties – SoD).

Parlare di sicurezza oggi vuol dire soprattutto garantire che ogni utente abbia accesso solo ai propri dati e solo alle funzioni di cui ha bisogno ed a cui è autorizzato. La limitazione all'accesso ai propri dati è generalmente ben visto e anzi richiesto dagli utenti, un po' meno la limitazione delle funzioni ma l'esperienza insegna che l'utente impara velocemente a lavorare solo con le funzioni di cui ha veramente bisogno.

D'altra parte, vi è una categoria di utenti che non è possibile gestire secondo questi criteri. E' ben noto, basta citare come esempi sia le norme specifiche del Garante della Privacy Italiano che le normative PCI, che gli amministratori di sistemi e applicazioni, per il ruolo ed i compiti a loro affidati, devono accedere con pieni privilegi. Di norma il concetto di Minimi Privilegi non si applica agli amministratori appunto perché per "gestire" sistemi ed applicazioni hanno bisogno di tutti i privilegi, mentre, come vedremo, in alcuni casi si potrebbe pensare di applicare in un qualche modo il principio della Separazione dei Compiti.

Dal punto di vista della sicurezza, questo è un problema non banale in quanto proprio gli utenti con maggiori privilegi e quindi a maggior rischio, sono quelli che risultano meno controllati e controllabili.

## Considerazioni Tecnologiche

Per entrare un poco più nel dettaglio di questa problematica, conviene partire dall'analizzare gli aspetti tecnologici in quanto non avrebbe molto senso considerare delle soluzioni quando poi queste risultassero non implementabili.

Possiamo dividere in tre principali fasi il lavoro amministrativo su un sistema od una applicazione (non ci addentreremo così tanto nei dettagli da avere necessità di distinguere fra di essi):

1. Accesso
2. Operatività
3. Tracciatura.

### Accesso

Ovviamente il primo e fondamentale momento nel processo amministrativo di applicazioni o sistemi ICT, è il momento dell'accesso alle applicazioni o sistemi da parte degli amministratori. E' chiaro che se gli accessi amministrativi fossero concessi facilmente o a chiunque, qualunque tipo di sicurezza verrebbe a mancare. Essendo una fase cruciale e la prima da affrontare, ne è risultato essere l'ambito in cui recentemente sono stati fatti i maggiori passi avanti. Pertanto sono abbastanza ben delineate delle procedure ideali da seguire per la gestione degli accessi amministrativi che ora riassumeremo.

Per prima cosa, un utente prima di essere un amministratore deve essere un utente normale dell'applicazione o del sistema. A parte applicazioni singole ed isolate ove questo per ora è raramente implementato, nel caso di applicazioni aziendali e di sistemi questo può essere implementato abbastanza semplicemente.

Il caso più comune è quello di una rete aziendale nella quale sia presente un dominio di autenticazione, ad esempio Active Directory, ove viene richiesto che ogni amministratore sia prima di tutto un utente normale non privilegiato del dominio, e come tale utente possa utilizzare i servizi di posta elettronica, navigazione web ecc. Per poter svolgere attività amministrativa, l'utente deve essere connesso alla rete come utente non privilegiato (ad eccezione del caso di operatività in emergenza descritta più avanti) e utilizzare questa autenticazione come primo passo per l'accesso amministrativo. Il secondo passo per l'accesso amministrativo può essere effettuato in varie modalità, le due più frequenti sono le seguenti.

L'utente si connette al sistema o applicazione che deve amministrare con la propria utenza non privilegiata, ed una volta connesso al sistema o applicazione esegue una seconda autenticazione per assumere i privilegi amministrativi. Questa soluzione non è però sempre implementabile e per ambienti molto estesi e variegati può portare ad una notevole complessità di gestione. In questo caso la soluzione ormai implementata da molti è quella di introdurre un sistema apposito di autenticazione e gestione delle connessioni amministrative.

Questi sistemi agiscono come dei Gateway implementando procedure simili alla seguente:

- identificazione dell'utente tramite le sue credenziali dell'utenza non privilegiata tipicamente di dominio
- opzionalmente richiesta di ulteriori credenziali anche di tipo One Time Password (OTP), biometriche ecc.
- richiesta del sistema o applicazione e dell'utenza che l'amministratore vuole utilizzare
- richiesta della motivazione, dell'attività da svolgere e dell'intervallo temporale previsto per lo svolgimento dell'attività
- fornitura di una connessione diretta e sicura all'utenza del sistema o applicazione senza bisogno di fornire ulteriori credenziali all'amministratore, oppure fornitura di credenziali One Time all'amministratore per permettergli di eseguire un accesso diretto.

Questi Gateway sono quindi un unico punto, e quindi critico, di accesso amministrativo a sistemi ed applicazioni e permettono di implementare politiche omogenee di sicurezza per tutti i sistemi e applicazioni, inclusi quelli legacy. Infatti in pratica è il Gateway che effettua l'autenticazione e l'assegnazione dei privilegi all'amministratore, incaricandosi di gestire le credenziali sui sistemi target, ad esempio i cambi password, e ove possibile le connessioni ai sistemi e applicazioni.

A parte abituare gli utenti amministrativi ad una nuova procedura di lavoro che alle volte può risultare non così immediata, questi Gateway introducono una nuova infrastruttura ed un nuovo livello di complessità nei sistemi ICT, che deve garantire la massima affidabilità perché è proprio nei momenti di crisi ed urgenza che gli amministratori hanno necessità di accedere a sistemi ed applicazioni. Inoltre non vanno sottovalutati i limiti di queste tecnologie e come al solito una buona pianificazione e configurazione può fare la differenza tra un sistema messo in sicurezza ed uno no.

Ad esempio va affrontato il tipico problema del trust amministrativo tra sistemi e applicazioni in modo da evitare, o permettere nel caso, che l'accesso amministrativo ad un sistema o applicazione non sia estendibile ad altri sistemi ed applicazioni, saltando (*hopping*) da uno all'altro mantenendo sempre i privilegi amministrativi.

Vanno inoltre considerate le procedure per le vere situazioni di emergenza, ad esempio quelle in cui i Gateway non funzionino, o vi siano dei problemi di connettività e l'accesso amministrativo tramite i Gateway ai device di rete (switch e router) risulti impossibile proprio perché la rete non funziona. Per questi casi bisogna predisporre delle procedure tipicamente manuali anche basate sulla identificazione fisica degli amministratori, che permettano di accedere ad esempio da console con privilegi amministrativi a sistemi e applicazioni.

## Operatività

Una volta in possesso di sistemi e procedure per identificare, autenticare ed autorizzare gli amministratori dei sistemi ed applicazioni, bisogna considerare la loro operatività. Su questo fronte invece non si sono fatti particolari passi avanti negli ultimi tempi. In pratica è abbastanza comune che quando un utente ha un accesso privilegiato ad un sistema od una applicazione, questi abbia tutti i privilegi ed accesso a tutti i dati. In alcuni, pochi, casi si fa distinzione fra amministratori (tutti i privilegi) ed operatori (un set limitato di privilegi ed accessi ai dati) soprattutto in grandi applicazioni. Ma nella maggior

parte dei casi risulta laboriosa e complessa da gestire l'implementazione di politiche di Minimi Privilegi e Separazione dei Compiti a livello tecnico.

Ad esempio per i sistemi operativi, sin dagli anni '80 sono presenti tecniche di controllo avanzato anche per privilegi amministrativi, che spesso vanno sotto il nome di *Mandatory Access Control*. E' possibile assegnare a ciascuna utenza esattamente i privilegi necessari per eseguire solo certe funzioni e limitare sia l'accesso che le modalità di accesso ai dati. Risulta però difficile gestire in maniera puntuale l'assegnazione dei privilegi e si finisce quasi sempre ad assegnare tutti o quasi tutti i privilegi agli amministratori, al più dividendoli in poche grandi classi.

Oggi il concetto e la pratica di amministratore di sistema è tipicamente quello di utenze con poteri assoluti, e non è detto che sia del tutto sbagliato.

## Tracciatura

La necessità di tracciare nel dettaglio le attività amministrative e privilegiate non è solo un requisito di leggi, normative e certificazioni, ma ha anche uno scopo preventivo, deterrente, di controllo, di allarme e forensico o di analisi a posteriori. In particolare, visto che i controlli tecnici preventivi sull'operatività degli amministratori sono tipicamente assenti, viene usualmente data particolare enfasi alla tracciatura delle attività con la produzione di allarmi e report di eventi di particolare importanza. In pratica invece che impedire le attività, le si tracciano in modo almeno da poter individuare, grazie ai controlli sull'accesso, chi ha fatto cosa.

Le soluzioni, spesso intere infrastrutture più che singole applicazioni, dette di *Security Information and Event Management* (SIEM) soddisfano queste esigenze, hanno attualmente buona popolarità e si sono sviluppate molto negli ultimi anni. L'implementazione di tali soluzioni non è però cosa facile, sia per la quantità di dati da trattare, che per le complessità tecniche da superare e per l'usuale problema di utilizzo da parte del personale. Infatti, come già accadeva anni fa per gli *Intrusion Detection System*, oggi superati spesso proprio per questi motivi dagli *Intrusion Prevention System*, è di ben poca utilità la produzione di allarmi e report che poi nessuno guarda e a cui non segua alcuna azione. Ovviamente non devono essere gli stessi utenti privilegiati a verificare gli allarmi e report generati sulla propria operatività, ma una terza parte tipicamente incaricata di attività di controllo operative quali le unità di Sicurezza Informatica, di Audit IT o di gestione dei Rischi, qualora queste siano presenti in azienda.

Un altro problema tecnico di difficile o complessa soluzione riguarda la possibilità per gli utenti privilegiati di modificare i log dei sistemi in modo tale da cancellare le traccie delle proprie attività. Ad esempio, un amministratore di sistema operativo in condizioni normali è in grado di modificare i log prodotti dal tracciamento delle proprie attività sul sistema, e quindi rendere difficile se non impossibile risalire sia al responsabile che ai dettagli dell'attività svolta. Vi sono ovviamente soluzioni tecniche che permettono la completa separazione tra attività privilegiate di amministrazione e tracciamento delle stesse, ma sono tipicamente implementate a livello operativo dai sistemi di Mandatory Access Control che come abbiamo visto, sono molto poco implementati.

## Considerazioni Procedurali

Se la tecnica ci permette di fare alcune cose per gestire in maggior sicurezza le attività degli amministratori, bisogna però considerare l'altra faccia della medaglia, ovvero l'aspetto della gestione del personale. Ovviamente il personale sistemistico e gli amministratori di sistemi ICT sono usualmente ben preparati tecnicamente e devono garantire affidabilità anche morale visto il ruolo che assumono all'interno dell'azienda.

Dato questo per scontato, il primo fattore da tenere in considerazione è che, con ben poche eccezioni, il personale sistemistico e gli amministratori di sistema sono sempre pochi in numero, nei migliori dei casi appena sufficienti a soddisfare le esigenze di gestione di sistemi e applicazioni. In questa situazione è d'obbligo che il personale venga organizzato in primo luogo nella maniera più produttiva per l'azienda. In pratica nella maggior parte dei casi questo significa gestire il personale per ruolo tecnico e secondo le competenze personali.

Ad esempio, tutti gli amministratori di basi dati (DBA) gestiscono ed hanno accesso intercambiabilmente a tutte le basi dati. Analogamente per gli amministratori di sistemi operativi Unix, Windows, di apparati di rete, firewall ecc. In questa maniera anche con poco personale si riescono a gestire grandi numeri di macchine, sistemi ed applicazioni.

Possiamo interpretare questa come una particolare implementazione del concetto di Separazione dei Compiti basata unicamente sulle competenze tecniche piuttosto che su principi di sicurezza e gestione dei rischi, mentre non vi è per nulla l'adozione di Minimi Privilegi. Se però consideriamo questa organizzazione dal punto di vista della gestione dei rischi e della sicurezza, la situazione è ben lontana dal-

l'essere ottimale.

Consideriamo il caso teorico, ma che spesso è anche reale, in cui gli amministratori di sistema abbiano accessi amministrativi a tutti i sistemi operativi, i DBA a tutte le basi dati, e gli amministratori di applicazioni a tutte le applicazioni. Se dal punto di vista tecnologico il ruolo di ognuno è ben definito e la divisione di compiti e responsabilità ben chiara, è necessario analizzare dal punto di vista del business i rischi per l'azienda associati alle attività privilegiate sui sistemi ICT. Guardiamo quindi dal punto di vista del business a cosa potrebbe fare un utente privilegiato, e a quali dati e processi aziendali ha accesso. Nel caso teorico indicato, sia un amministratore di sistema che un DBA che un amministratore di applicazioni ha accesso a tutti i dati ed a tutti i processi dell'azienda. Un qualunque utente privilegiato potrebbe quindi realizzare processi e modificare i dati a suo piacere, violando qualunque basilare logica di controllo aziendale di business.

Ad esempio, è normale logica aziendale che chi emette un ordine verso un fornitore non sia anche abilitato ad autorizzare il pagamento della relativa fattura. La Separazione dei Compiti nella gestione dei rischi aziendali è vista all'interno dei singoli processi di business proprio per garantirne la correttezza introducendo opportuni controlli. Da questo punto di visto la virtuale “Separazione dei Compiti” degli utenti privilegiati ICT appena descritta, adotta una logica del tutto ortogonale a quella di business ed affida in pratica ad una spesso fantomatica tracciatura delle attività privilegiate il compito di garantirne la correttezza.

Il problema non è ignoto e spesso viene sollevato quando si valutano i controlli esistenti nell'ambito dell'analisi dei rischi di business aziendale. Quando si valutano i privilegi e la separazione dei compiti degli utenti dei sistemi ICT, se si considerano anche le utenze amministrative, queste tipicamente violano ogni politica aziendale. Si preferisce quindi non considerarle da questo punto di vista, ma il problema ed i rischi associati sono reali.

Bisogna infatti anche valutare lo scenario in cui, per una qualunque ragione anche tecnica, oltre ad un dipendente infedele che intenda fare una frode interna, anche un individuo esterno non autorizzato possa accedere ai sistemi con privilegi amministrativi. Come esempio estremo si può sempre pensare a cosa potrebbe succedere in questo caso in un sistema di Internet Banking. L'assenza di una vera separazione dei compiti e limitazione dei privilegi per le utenze privilegiate, implica che nel caso di utilizzo fraudolente di una di queste, i danni e le conseguenze possibili per l'azienda sono estremi e non è detto che i sistemi di controllo accessi e tracciatura delle attività implementati siano in grado di limitarli in

modo efficace.

L'accettazione conscia di questi rischi da parte dell'azienda o, come purtroppo capita troppo spesso, l'ignorarli completamente, sono comunque delle soluzioni insoddisfacenti visti il ruolo e la basilarità delle funzioni in considerazione. Non è chiaro se qualche soluzione tecnica potrà in futuro aiutare a gestire meglio queste problematiche, anche perché il problema principale è proprio nella relazione tra i rischi tecnici ICT e quelli aziendali di business, che in questo caso risultano spesso più ortogonali che allineati.

In conclusione, la problematica della gestione delle utenze privilegiate e delle attività amministrative di sistemi ed applicazioni, è complessa sia dal punto di vista tecnico che di gestione ed organizzazione del personale. Le necessità di sicurezza e gestione dei rischi aziendali di business soprattutto in questo caso si scontrano con le esigenze, molto vive in questo periodo, di efficienza organizzativa e di dolorosi tagli di budget, che obbligano a concedere al poco personale ICT privilegiato totale accesso ai dati e processi di business anche in violazione delle politiche di sicurezza aziendali.

Andrea Pasquinucci (PhD CISA CISSP, socio AIEA) è un consulente freelance in sicurezza informatica. Si occupa prevalentemente di progetti di sicurezza ICT, audit, compliance, governance e formazione ICT per il management ed il personale tecnico. In particolare è esperto di sicurezza delle reti e dei servizi web, dei sistemi operativi e di crittografia.