ANALISI
8 Maggio 2011

HSPI

ACCESS CERTIFICATION
UN APPROCCIO COMPLEMENTARE ALL'IDENTITY & ACCESS MANAGEMENT

Ing. Corrado Pomodoro, Information Risk Management, Senior Manager HSPI

L'informatizzazione dei processi aziendali, la diffusione dei servizi on-line e delle tecnologie collaborative, l'incremento costante del numero di soggetti che, a vario titolo, utilizzano i dati dell'azienda, rende sempre attuale e centrale uno dei controlli più "anziani", seppure mai sufficientemente consolidati, nell'ambito della sicurezza delle informazioni: il controllo delle identità e degli accessi alle applicazioni ed ai sistemi.
Le soluzioni esistenti sono tante e diversificate. Uno dei paradigmi risolutivi più completi e strutturati che si è andato evolvendo e consolidando nel corso degli anni è quello dell'Identity & Access Management (I&AM) basato sul modello RBAC (*Role Based Access Control)*.
D'altra parte, i progetti di implementazione di piattaforme I&AM che si integrano con tutti i sistemi informativi consentendo di disciplinare l'accesso a tutti i dati aziendali richiedono sforzi economici ed organizzativi molto rilevanti.
In un panorama industriale di aziende prevalentemente di dimensioni medio-piccole, in una congiuntura di mercato in contrazione e con la prospettiva di continua evoluzione dei sistemi informativi nonché degli attori coinvolti nella loro gestione (outsourcing), tali sforzi si rendono di difficile intrapresa, spesso difficilmente giustificabili ed ancora più spesso avviati e non portati a termine.
Inoltre, spesso l'adozione di piattaforme I&AM viene fatta a macchia di leopardo, lasciando così delle brecce, dei vuoti di gestione, che in un mondo informatico ormai totalmente interconnesso, rappresentano delle vulnerabilità che non possono essere trascurate.
La consapevolezza dei limiti del modello I&AM "classico", il consolidamento di best practice, l'evoluzione delle tecnologie per la gestione delle identità stanno promuovendo la diffusione di un nuovo modello complementare ed "elastico", che consente un approccio organico rispetto alle diverse strutture organizzative dell'azienda e trasversale ai diversi sistemi informativi. Il modello di cui parliamo indirizza la verifica delle identità digitali, assicurandone – a monte – il rispetto dei criteri di autorizzazione e può essere applicato sia dove la completa automazione del flusso operativo di definizione, profilazione e provisioning (obiettivi dell'I&AM) potrebbe essere troppo onerosa, sia dove gli obiettivi di controllo sono rallentati e in alcuni casi impediti dalla difficoltà di comprendere a pieno e bonificare le situazioni esistenti.
Al fine di introdurre e illustrare meglio il modello, faremo una breve analisi delle problematiche tipiche della gestione delle identità e del controllo degli accessi.

Il problema della proliferazione delle identità digitali nelle organizzazioni complesse

Nelle organizzazioni complesse e non solo, esistono molti sistemi applicativi nati e sviluppati su piattaforme diverse, in epoche diverse, con strutture più o meno flessibili e standardizzate. Ci sono, per esempio, applicazioni che prevedono l'autenticazione basata su Directory Services (es. LDAP o Active Directory) o su file "users" interni all'applicazione stessa; applicazioni che consentono la configurazione di profili di accesso dall'esterno oppure che prevedono profili autorizzativi cablati nel codice.

Le ragioni della disomogeneità sono diverse e vanno dalla mancanza di policy e/o standard ben definiti e conosciuti, ad oggettive difficoltà tecniche o di aggiornamento, ai diversi livelli di importanza e/o criticità per il core business dell'organizzazione.

Quali siano gli impatti di una situazione simile è spesso di difficile determinazione, ma possiamo abbozzare una lista di effetti indesiderati:

- necessità di replicare la definizione degli utenti sui diversi sistemi;
- difficoltà di tracciamento delle identità associate allo stesso utente;
- disallineamento degli account rispetto agli effettivi utenti autorizzati (es. esistenza di abilitazioni per utenti non più in azienda);

- disallineamento dei profili configurati rispetto alle necessità del ruolo ricoperto;
- possibilità di conflitti di competenze.

Il problema dei ruoli e dei profili

Prima di tutto un po' di chiarezza sui termini. Senza la pretesa di stabilire delle verità assolute, vogliamo, almeno per la durata di questo articolo, stabilire delle coordinate di riferimento utili per comprendere cosa intendiamo.

Quando diciamo identità digitale, ci riferiamo al cosiddetto "account" composto di username e password; la username è ciò che contraddistingue un'identità digitale da un'altra.

Quando diciamo "ruolo", ci riferiamo ai compiti e alle funzioni assegnate ad un utente in quanto parte dell'organizzazione. Un ruolo può quindi essere, per fare qualche esempio, quello del Responsabile degli Acquisti o quello dell'Operatore di Database o, ancora, quello del Responsabile della Sicurezza.
Si tratta di figure alle quali l'organizzazione assegna delle precise mansioni, ovvero l'insieme delle stesse mansioni.

Il problema dei ruoli è dunque un problema di responsabilità delle Risorse Umane / Organizzazione.

Quando diciamo "profilo", ci riferiamo invece all'insieme di abilitazioni che caratterizzano le autorizzazioni di accesso di una determinata "identità digitale", vale a dire una username con la sua password.

Di chi sia *il problema della definizione dei profili, rispetto a quella dei ruoli, è questione ben più dibattuta.*
Le best practice sostengono che i profili di autorizzazione debbano essere assegnati dagli owner dei servizi, da coloro cioè che hanno responsabilità "accountable" (responsabilità ultima) sui servizi erogati attraverso determinate applicazioni e sistemi informativi. Nella realtà questa responsabilità è purtroppo spesso declinata a favore degli amministratori dei sistemi informativi e dei loro responsabili.

La realizzazione di un sistema RBAC, che è uno degli obiettivi primari di una soluzione I&AM, consente la definizione di profili disaccoppiati dall'utente specifico, ma assegnati in base al ruolo che l'utente assumerà per l'organizzazione.

L'entropia delle identità digitali

La gestione delle identità digitali include sempre, ma non si esaurisce in essi, due momenti fondamentali: il primo consiste nella creazione delle credenziali, costituite da una username e da una password (semplice, strong, biometrica o quanto di più esoterico); il secondo consiste nell'associazione dei diritti di accesso/abilitazioni alle identità create.

Sono queste due azioni che creano, nella maggior parte delle realtà, un'entropia da cui, dopo qualche tempo è difficile e costoso districarsi.
Con quale criterio sono definite le stringhe di caratteri che compongono la username (nome, iniziali, CF, matricola, …)? Con quale criterio sono assegnate agli utenti (una username per utente, molte username per utente, …)? In quanti sono autorizzati a definire le identità?

E … siamo solo alla prima azione. Con la seconda il disordine sovrano è assicurato.
Chi definisce o modifica le abilitazioni? Chi le autorizza? Chi le controlla e quando? Chi verifica che non siano in conflitto? Chi verifica se e come siano utilizzate?

Il processo, come dicevamo, nella maggior parte dei casi è entropico. Le cosiddette "change request" in questo ambito sono all'ordine del giorno; il change management, in molte realtà, uno sforzo sovrumano.

Le tecnologie attuali: virtù e limiti

Come abbiamo già detto da molti anni esistono sul mercato soluzioni e tecnologie per la gestione delle identità digitali e il controllo degli accessi, note con il termine di Identity & Access Management.

Gli istituti di ricerca ne recensiscono diverse tra le quali: Oracle, Novell, IBM, Computer

Associates e diverse altre. Si tratta in molti casi di soluzioni modulari che includono molte utili funzionalità:

- directory Service: i DB, fisici o virtuali, che centralizzano le identità digitali;
- connettori: sw specializzati per i diversi target applicativi che consentono l'automazione del provisioning, vale a dire la configurazione delle identità digitali e dei loro profili all'interno delle applicazioni di cui si intende gestire il controllo degli accessi;
- motori di workflow: sistemi che supportano la gestione del flusso autorizzativo di provisioning;
- Single Sign On: funzionalità di disintermediazione dell'accesso che consente l'affrancamento per gli utenti dall'uso di molteplici password;
- federation: supporto di protocolli standard per stabilire relazioni di fiducia tra domini di autenticazione;

ed altre.

Come anche abbiamo già detto le tecnologie di cui parliamo, hanno avuto nei recenti anni notevoli sviluppi e si trovano attualmente in una fase che potremmo definire di maturità.

Ciononostante il successo di una realizzazione I&AM dipende solo parzialmente dalla maturità tecnologica. L'introduzione dei meccanismi di automazione di cui abbiamo parlato, sebbene possa produrre straordinari benefici, impone spesso dei cambiamenti organizzativi che difficilmente possono essere promossi e sostenuti dalla direzione Sistemi Informativi. Senza una forte sponsorizzazione ed un commitment coerente da parte delle direzioni di Business e Risorse Umane/Organizzazione un progetto I&AM avrà ottime probabilità di insuccesso, senza contare il costo elevato dei software e delle infrastrutture necessarie.

Gli impatti, economici ed organizzativi, sono tanto meno trascurabili quanto più è esteso il perimetro di applicazione della soluzione. Questo obbliga nella maggior parte dei casi a restringere il target alle cosiddette applicazioni "core" o a quelle considerate più critiche per ragioni di compliance o più strettamente di business o, in altri casi al perimetro consentito da ragioni di budget e/o di fattibilità organizzativa. Lasciando il "resto del mondo" non presidiato.

Una situazione del genere, fortemente disomogenea tra ciò che è nel perimetro I&AM e ciò che non lo è, presenta oltre che una pericolosa vulnerabilità, tutti i difetti di una doppia gestione.

Access Certification

Access Certification o, all'italiana, la certificazione degli accessi, è un sistema per assicurare omogeneità nella gestione delle identità e delle abilitazioni ed eliminare "vuoti" di controllo.

Con Access Certification intendiamo un processo con il quale un gruppo di responsabili accreditati revisiona, periodicamente o quando necessario, chi ha accesso a cosa al fine di confermare, revocare o modificare i diritti di accesso opportunamente e in coerenza con le policy e/o i requisiti di business.

Il processo, seppure in linea teorica sia fattibile manualmente, nelle situazioni che abbiamo descritto all'inizio di questo articolo, con molti sistemi e applicazioni diversificati e gestiti in modo disomogeneo, può comportare un elevato dispendio di risorse se non supportato da adeguate soluzioni tecnologiche.

Le soluzioni – processo e strumenti - per via del loro minore impatto sia in termini economici che organizzativi, possono essere attuate su un perimetro ben più ampio di quello indirizzato da una soluzione I&AM.

Sia ben chiaro, non si tratta di un'alternativa o di una soluzione di compromesso, ma piuttosto di un controllo che può essere definito "compensativo". Un controllo cioè che consente la gestione di un rischio non accettabile laddove le migliori contromisure

non siano attuabili o lo siano solo parzialmente, complementandole e/o sostituendole.

Peraltro non può neanche considerarsi un ripiego o una soluzione di compromesso. Si tratta di una prassi corretta di controllo *adeguato al livello di rischio*, il che presuppone per la sua applicazione una valutazione dei rischi e degli impatti (ma questo sarà oggetto di un prossimo approfondimento).

Vediamo alcune caratteristiche e benefici di una soluzione di Access Certification:

- raccolta automatizzata delle identità e delle loro abilitazioni dai sistemi target;
- aggregazione e normalizzazione delle identità collezionate;
- presentazione delle identità e delle abilitazioni in un linguaggio "business" comprensibile a chi per competenza dovrebbe autorizzare;
- impostazione guidata delle policy o regole di base (nei confronti delle quali verranno confrontate le abilitazioni esistenti) come, ad esempio, le policy di separazione dei compiti (SOD) e di privilegio minimo (Need to know);
- identificazione ed evidenziazione delle situazioni anomale o di rischio e delle relative azioni correttive, come: violazione delle policy, concentrazione eccessiva di diritti su uno stesso utente, cambiamenti significativi sulle abilitazioni, identità "orfane", etc.;
- prioritizzazione e focalizzazione delle azioni in base all'effettivo rischio di business;
- modifica, disabilitazione o cancellazione senza bisogno di tecnologie di provisioning;
- impostazione ed automazione di un ciclo di verifica coerente con le necessità operative;
- tracciamento di tutte le attività di verifica e reportistica di dettaglio.

Una soluzione di Access Certification è di norma progettata per essere utilizzata sia da coloro che sono preposti alla sicurezza delle informazioni (Security administrator) che dai rappresentanti delle funzioni di business.

La soluzione oltre che con le piattaforme di I&AM, quando presenti, si integra e offre i massimi benefici con strumenti di Data Loss Prevention (DLP), Security Information Event Management (SIEM) o sistemi di logging. Tali strumenti – DLP e SIEM – supportando rispettivamente la localizzazione dei dati sensibili sui vari sistemi e l'individuazione di attività sospette, contribuiscono alla identificazione degli utenti o delle identità digitali che rappresentano maggiori rischi per l'organizzazione. Combinando questi dati con quelli relativi ai profili configurati nei sistemi le soluzioni di Access Certification assicurano un efficace strumento di supporto alle decisioni e alla rapidità di reazione.

Un'ultima, ma non meno importante, notazione: una soluzione di Access Certification dovrebbe, a nostro avviso, precedere qualsiasi implementazione di I&AM in quanto l'azione di bonifica e di analisi delle identità ed abilitazioni esistenti ottenuta attraverso il processo di Access Certification, offre notevoli vantaggi per una progettazione ottimale ed ottimizzata della soluzione I&AM. Ciononostante, per le realtà che hanno già avviato ed investito in progetti di I&AM, l'Access Certification offre la possibilità non solo di ampliare il perimetro dei controlli, ma anche di accelerare i processi di transizione verso il modello RBAC (Role Based Access Control) attraverso una gestione più consapevole e razionalizzata delle identità e dei profili, rendendo il sistema più efficace nel suo complesso.

Le soluzioni tecnologiche in questo ambito non sono molte attualmente; possiamo citare senza essere esaurienti alcuni prodotti come: Novell Access Certification Manager, Computer Associates Role and Compliance Manager, Courion, SailPoint. Ma il numero dei prodotti, le loro funzionalità e le possibilità di integrazione, così come la loro

connotazione e consolidamento nel mercato sono in netto aumento.

Conclusioni

Il tema della gestione delle identità e del controllo degli accessi agli asset informativi è in continua evoluzione e reso sempre più attuale dal deciso aumento dei rischi oltre che dagli obblighi di compliance.

Il tema può essere declinato in molteplici fattori e tipologie di controllo. I controlli più automatizzati e in tempo reale, costituiti dalle piattaforme I&AM, per via dell'elevato impatto economico ed organizzativo vengono, all'atto pratico, impiegati su perimetri ristretti e spesso a macchia di leopardo con riduzione di efficacia. Inoltre, la transizione verso i modelli RBAC che, come dicevamo è uno degli obiettivi primari delle soluzioni I&AM, è rallentato e in alcuni casi impedito dalla difficoltà di bonificare le situazioni esistenti.

L'Access Certification, come insieme di processi e tecnologie, rappresenta un efficace meccanismo di controllo che consente alle organizzazioni, attraverso un regolare e semplificato ciclo di verifica e validazione dei privilegi di accesso degli utenti, di ridurre drasticamente le situazioni di non conformità e l'esposizione al rischio.

HSPI SpA - Consulenti di Direzione
Via Guido Reni 2/2 - 40125 Bologna (Italy)
P.IVA 02355801206

Tel. +39 051 2960545 | Fax. +39 051 6568695
BOLOGNA | MILANO | ROMA
www.hspi.it | e-mail: info@hspi.it