La Gestione delle Identità nelle aziende

Ludovica Esposito & Marco Giovinazzi, Bull Italia Security Competence Center

Abstract— **La Gestione delle Identità (Identity Management, o IM nel seguito) dei dipendenti all'interno delle grandi aziende costituisce un tema attuale e destinato ad essere affrontato da molte realtà produttive.**
L'approccio della nostra relazione sull'IM è essenzialmente pratico: descriveremo, in base alla nostra solida esperienza come system integrator, focalizzato sulla sicurezza dei sistemi informativi, come può essere affrontato un progetto di realizzazione di un sistema di IM, all'interno di una grande e complessa azienda con un numero elevato di dipendenti e un articolato sistema informativo.
In particolare approfondiremo i seguenti quesiti: cosa è in effetti un sistema di IM? Quali sono gli obiettivi che devono essere raggiunti dall'azienda che ne realizza uno al proprio interno? Cosa e come bisogna fare per centrare tali obiettivi? Quali sono le principali difficoltà tecniche ed organizzative che si incontrano? Quali sono le più frequenti problematiche di gestione e manutenzione di un sistema di IM?

Queste "linee guida" possono essere considerate i nostri personali appunti di lavoro, quelli che usiamo per rinfrescare le idee quando un nuovo sistema di IM deve essere proposto ad un Cliente e quindi progettato ed iniziato, e che ora mettiamo a disposizione del pubblico di Net&System Security 2006.

I. Introduzione

Definizioni - L'*Identity Management* è una vasta area amministrativa che tratta dell'identificazione degli individui all'interno di un sistema (come un paese, una rete o un'impresa) e del controllo accessi alle risorse al suo interno. Tale controllo è basato sull'associazione dell'identità ad un adeguato insieme di diritti d'accesso e restrizioni[1].
Nell'ambito di un'organizzazione l'Identity Management System è dato dall'integrazione di politiche, processi e tecnologie atte a gestire in modo centralizzato l'accesso degli utenti alle diverse risorse ed applicazioni informatiche, ed a proteggere così le informazioni da abusi da parte di utenti non autorizzati
Tipicamente il software di Identity e User Management è usato per centralizzare e automatizzare compiti amministrativi, come la reimpostazione delle password degli utenti o la generazione di credenziali di accesso a piattaforme ed applicazioni di business.

[1] Un semplice esempio di gestione delle identità è offerto dal sistema delle patenti di guida nel quale i guidatori sono identificati dal numero della patente e le eventuali limitazioni d'uso (come "interdizione di guida notturna") sono associate al numero identificativo.

In un contesto più vasto, consorzi formati da industrie e gruppi di lavoro indipendenti (Eclipse, W3C, The Open Group), stanno sviluppando gli standard che dovrebbero rendere possibile la gestione globale delle identità, attraverso la quale ciascuno di noi sarebbe identificato in modo univoco e reso in grado di gestire personalmente tutti i propri dati. Diversi sottoinsiemi dei dati personali potrebbero essere resi accessibili a soggetti esterni (dalla banca all'ufficio delle imposte, dal sistema sanitario nazionale all'internet service provider, ecc) in base ai servizi richiesti e alla necessità di riservatezza.
Ambito – Nel seguito di questo articolo concentreremo l'attenzione sulle tematiche specifiche della gestione delle identità all'interno di aziende di medie e grandi dimensioni.

II. Obiettivi e Caratteristiche

Obiettivi - La realizzazione di un sistema di IM all'interno di un'organizzazione è finalizzata al raggiungimento di un aumento del controllo, della produttività e della sicurezza ed alla riduzione dei costi di gestione delle utenze. Inoltre alcune delle funzionalità offerte da un sistema di IM possono risultare ottimi strumenti per ottenere la conformità alle norme vigenti in materia di sicurezza delle informazioni.

Funzionalità e caratteristiche che consentono di raggiungere gli obiettivi -
L'*aumento del controllo* si ottiene mediante l'introduzione di uno strumento centralizzato di attribuzione e gestione delle credenziali di accesso ai vari sottosistemi (rete, applicazioni, servizi), dotato di funzionalità di auditing (la creazione, modifica e cancellazione delle credenziali viene registrata con orario ed autore della modifica). In questo senso l'IM rappresenta lo strumento unico nel quale sono immediatamente individuabili tutte le informazioni relative ai diritti di accesso di un utente sui vari sottosistemi, comprensive di storico.
L'*aumento della produttività* può essere ottenuto grazie alla riduzione dei tempi di approntamento e modifica degli strumenti di lavoro informatici (credenziali di accesso ai diversi sistemi) per i singoli utenti. Il vantaggio è particolarmente evidente all'atto dell'inserimento di una nuova persona nell'organizzazione: in molte realtà ciò può comportare un'attesa di giorni, non solo perché la creazione degli account deve avvenire localmente su ciascun sistema, ma anche perché ad ogni sistema corrisponde un diverso amministratore, che deve essere opportunamente autorizzato per agire. Con l'IM invece è tutto automatico ed immediato poiché il workflow di autorizzazione viene integrato nel sistema e la generazione dei diversi account è contemporanea ed estremamente semplice.
All'*aumento della sicurezza* contribuiscono diversi elementi, come l'eliminazione gli account zombie, tipica della fase

iniziale dell'esercizio del sistema di IM, l'eliminazione dei ritardi nella revoca degli account in caso di dimissioni e delle inconsistenze tra livelli di autorizzazione dei diversi account di una stessa persona, l'associazione di tutti gli account di servizio a persone identificate e l'applicazione di politiche centralizzate alle password (cfr. nel seguito "password syncronization" e "SSO").

La *riduzione dei costi di gestione delle utenze* è ottenuta mediante la centralizzazione (e se possibile, l'automazione) delle operazioni di gestione sui diversi sottosistemi coinvolti: l'amministratore di sistema non deve più svolgere compiti ripetitivi su più sistemi diversi ma crea/modifica/elimina tutti gli account necessari ad una persona con un'unica operazione. Inoltre, se presente, la funzionalità di self service reset della password consente di ridurre le chiamate all'help desk per problemi di accesso (password dimenticate).

Analogo risparmio di risorse potrebbe essere ottenuto implementando la funzionalità di "*password syncronization*". In tal modo la modifica della password effettuata su un singolo account viene propagata su tutti gli altri account associati all'utente, riducendo il numero di password da memorizzare ed eliminando il problema dei "post-it" attaccati sui monitor. Tuttavia non c'è convergenza di opinioni circa l'aumento di sicurezza che la password syncronization porterebbe, in quanto ad un eventuale malintenzionato basterebbe indovinare una password per ottenere tutte le informazioni accedibili dall'utente sui vari sistemi. Inoltre questa scelta comporta problemi di integrazione poichè su ciascun sottosistema inserito nell'IM deve essere implementato uno strumento che intercetti la nuova password all'atto della modifica e la propaghi verso gli altri sottosistemi ("password interceptor"). Infine devono essere considerati gli impatti sulle prestazioni del sistema che possono aver luogo, in realtà di grandi dimensioni, se molte modifiche di password vengono effettuate contemporaneamente in orari di punta.

Una valida alternativa alla password syncronization è il *Single Sign On Sicuro*, nel quale l'utente effettua l'autenticazione primaria mediante autenticazione forte (es: smart card) mentre le credenziali per l'accesso ai sottosistemi sono gestite dal SSO. Il SSO viene spesso associato all'IM, anche se non ne è parte integrante, risulta particolarmente soddisfacente per l'utente finale ed offre buone caratteristiche di sicurezza.

Le *norme vigenti in materia di sicurezza delle informazioni* richiedono garanzia di riservatezza delle informazioni sensibili mediante applicazione del controllo degli accessi, e tracciabilità delle operazioni effettuate sui sistemi. In questo senso l'IM offre una visione organica ed immediata degli accessi consentiti alle informazioni, risolve le eventuali inconsistenze tra i diversi sistemi, offre strumenti di logging ed auditing.

III. Principali tematiche di sviluppo e Gestione

La realizzazione di un sistema aziendale di IM è un tipico compito da system integrator; dal punto di vista architetturale l'IM è uno strato software che deve essere posto al di sopra dei sottosistemi di sicurezza di tutti gli applicativi aziendali. Alcune delle principali tematiche di sviluppo e gestione sono indicate nel seguito.

Dati – E' necessario stabilire quale insieme di attributi definisce un'identità all'interno dell'organizzazione e risolvere le disomogeneità provenienti dall'integrazione di diversi sottosistemi. Il tema dei dati continua ad essere centrale durante tutto il ciclo di vita del sistema di IM che è soggetto a continue evoluzioni derivanti dalla progressiva inclusione di nuovi sottosistemi da gestire.

Sicurezza – A causa dell'elevata sensibilità dei dati trattati dall'IM (dati personali dei dipendenti, password, dati di auditing, etc), nella progettazione deve essere posta particolare attenzione alla scelta dei meccanismi di sicurezza. Tra le tematiche relative alla sicurezza ricordiamo la scelta del tipo di autenticazione per il personale che gestisce l'IM, la cifratura dei canali di comunicazione tra componenti del sistema (server, agenti, console amministrative, basi dati) e l'unificazione delle politiche applicate alle password sui vari sottosistemi.

Organizzazione – Per consentire l'inizio del funzionamento del sistema di IM devono essere definite le figure professionali deputate alla gestione e le relative strutture, e deve essere definito il processo per la richiesta di creazione e gestione delle utenze. Inoltre il sistema deve essere incluso nella struttura di Help Desk con le opportune procedure di intervento.

Aspetti legali – Particolare attenzione deve essere riservata agli aspetti legali relativi alle informazioni trattate (es: le identità dei dipendenti che cessano il rapporto di lavoro non possono essere cancellate realmente, ma devono essere solo disattivate, richiedendo la legge che i dati di autiding relativi agli accessi a certe informazioni siano conservati per un determinato periodo).

Evoluzioni – Poiché l'IM è intrinsecamente soggetto ad evoluzioni continue, causate dalla progressiva introduzione di nuovi sistemi ed applicativi, le aziende che si dotano di questo strumento si trovano a dover superare la rigidità della separazione tra sviluppo ed esercizio, e necessitano di una stretta collaborazione tra le due funzioni per tutto il ciclo di vita dell'IM.

IV. Conclusioni

L'introduzione di un sistema di gestione delle identità nel sistema informativo di un'organizzazione è finalizzata all'aumento della sicurezza e della produttività.

L'implementazione di un tale sistema è compito tipico da system integrator; in effetti, gli aspetti tecnici più onerosi da affrontare nello sviluppo sono legati all'integrazione di diversi sistemi preesistenti.

Aspetti legali ed organizzativi costituiscono una parte consistente del lavoro di realizzazione dell'IM.