

IDENTITY AND ACCESS MANAGEMENT: LA DEFINIZIONE DI UN MODELLO PROCEDURALE ED ORGANIZZATIVO CHE, SUPPORTATO DALLE INFRASTRUTTURE, SIA IN GRADO DI CREARE, GESTIRE ED UTILIZZARE LE IDENTITÀ DIGITALI SECONDO QUANTO PREVISTO DALLE POLICY DI BUSINESS E DALLE NORMATIVE

In un contesto in cui si moltiplicano le riorganizzazioni aziendali e aumenta costantemente l'esigenza di conformità a leggi, normative e standard, accompagnato da un ambito tecnologico sempre più complesso, è fondamentale mantenere la regolamentazione e il controllo delle credenziali degli utenti e del controllo accessi andando ad identificare e gestire ciò che viene definita "Identità Digitale".

Il Sistema IAM fornisce una serie di servizi a supporto per la Gestione delle Identità Digitali. Per realizzare un progetto di Identity and Access Management occorre un approccio metodologico che consenta di partire dall'analisi della situazione esistente, dei requisiti normativi e degli obiettivi di sicurezza fino ad arrivare ad una strategia implementativa della soluzione. Spike Reply realizza progetti di Identity and Access Management sfruttando una metodologia proprietaria in grado di adattarsi alle specifiche esigenze del Cliente e verificata con il best of breed delle soluzioni tecniche disponibili sul mercato.

LA TEMATICA

L'incombente crisi economica sta enfatizzando due fenomeni ben noti: da un lato le frequenti riorganizzazioni aziendali e dall'altro un generale malcontento dei dipendenti o di coloro che vengono estromessi dall'Azienda. Per controllare il fenomeno e ridurne l'impatto, le principali Istituzioni aumentano continuamente i controlli di conformità a leggi, normative e standard. Lo scenario si completa con un ambito tecnologico sempre più complesso in cui diventa difficile mantenere il controllo.

Date queste premesse, è fondamentale mantenere la regolamentazione e il controllo delle credenziali degli utenti e del controllo accessi andando ad identificare e gestire ciò che viene definita "Identità Digitale". Infatti, dal momento che l'implementazione tradizionale di una policy aziendale di sicurezza consiste nella definizione di un reticolo di permessi assegnati a determinati utenti, il processo con cui le loro identità vengono gestite (creazione, modifica, eliminazione) e con cui vengono loro assegnati specifici permessi, è la base, spesso trascurata, su cui si fonda la sicurezza dell'intero sistema informativo.

Nello scenario precedentemente descritto, la problematica della gestione degli utenti cresce ulteriormente quando calata nelle specificità tecnologiche delle singole realtà aziendali: un insieme eterogeneo di applicazioni e ambienti di lavoro che interagiscono poco o nulla tra loro, ognuno con il proprio sistema di autenticazione e con un proprio repository delle identità.

Questa situazione si traduce facilmente:

- nella necessità da parte degli utenti di autenticarsi con credenziali differenti a ciascuna applicazione, caricandoli della necessità di ricordare numerose combinazioni di username e password;
- nell'aumento del carico di lavoro del personale IT a causa della necessità di dover impiegare, per la gestione degli utenti di ogni applicazione, strumenti, procedure e policy differenti;
- nell'aumento del carico di lavoro dell'Help Desk impegnato a supportare gli utenti che si scordano le loro credenziali di accesso o la corretta applicazione delle policy;
- nella diminuzione del livello generale della sicurezza in quanto tutta l'architettura, generalmente, viene resa il più semplice possibile ed allineata al servizio con il livello di sicurezza più basso;
- nell'impossibilità di rispettare requisiti normativi: spesso, la complessità di tali processi non permette il rispetto di eventuali requisiti normativi aziendali o dettati da enti governativi esterni.

LA SOLUZIONE

Con Identity and Access Management si indica l'intero processo (applicazione di policy appropriate ed impiego di strumenti tecnologici) per gestire le informazioni riguardanti l'identità degli utenti e controllarne l'accesso alle risorse aziendali.

Da un punto di vista tecnologico, nel termine IAM è consuetudine far confluire i Repository centralizzati dove sono depositate le identità digitali (Enterprise Directory Services) e i Servizi tecnologici che ne consentono la Gestione. Gli obiettivi della soluzione IAM sono i seguenti: aumentare la produttività e la facilità d'uso del sistema informatico da parte degli utenti finali, aumentare il livello generale della sicurezza, diminuendo i costi associati alla gestione degli utenti e delle loro identità, dei loro attributi e delle loro credenziali. In sintesi, ci si propone di realizzare uno strumento che supporti il processo che stabilisce chi ha accesso a quali risorse, l'assegnazione delle autorizzazioni, la loro modifica o revoca quando necessario, nonché la gestione del processo stesso ed il monitoraggio delle attività, nel rispetto delle politiche aziendali di sicurezza.

Lo IAM non è quindi una soluzione chiavi in mano, ma una strategia di business che si traduce nell'implementazione di un complesso di soluzioni che coinvolgono l'intera organizzazione: lo IAM è un insieme di tecnologie e processi di business. Per questo motivo non esiste un singolo approccio alle problematiche di Identity and Access Management, in quanto la strategia implementativa deve rispecchiare per ogni organizzazione gli specifici requisiti di business ed il relativo contesto tecnologico.

IL MODELLO TECNOLOGICO. Il modello tecnologico a supporto dei Processi IAM si divide in quattro pilastri principali: i Servizi di Identity Management, i Servizi di User Provisioning, i Servizi di Access Management e i Servizi di Single Sign On. Questi pilastri sono alimentati dalle funzioni di Policy Management e Audit e devono essere accompagnati da Servizi di Alta Disponibilità, Scalabilità e Distribuzione.



Comprendono le soluzioni tecniche modulari, adottabili in singoli componenti o parte di suites complete.

I componenti sono:

- Identity Management
- ID Synchronization
- User Provisioning
- Workflow
- User Self Service
- Audit and Reporting
- Compliance e Role Management
- Enterprise Single Sign On
- Strong Authentication
- Web Access Management
- Federation Services.

IL PROGETTO IAM

Spike Reply supporta le aziende/organizzazioni in tutte le fasi del “Progetto IAM” che può essere articolato nelle seguenti attività:

IL MODELLO PROFILATIVO. Il primo passo fondamentale nel processo di sviluppo ed implementazione di una soluzione di IAM è comprendere quali siano i principali requisiti di business, identificando i processi chiave, le applicazioni critiche e tutte le informazioni necessarie per rispettare gli obiettivi di business. Una parte molto importante di questa fase di analisi prevede che l’organizzazione aziendale debba definire quali utenti devono accedere a quali risorse e con quale livello di sicurezza. Questa fase di analisi per molte aziende può rivelarsi un’ottima opportunità per rivedere politiche e processi interni non proprio efficienti. Il risultato atteso di questa fase è la definizione di un modello di profilazione e la mappatura dei processi amministrativi.

GESTIONE DEI PERMESSI E DELLE POLICY. Al centro di ogni strategia di IAM si pone la necessità di stabilire un insieme di permessi e di policy di sicurezza e di assicurarne l’applicazione in tempo reale. Molte organizzazioni hanno scoperto che il modo migliore per garantire un’efficace gestione delle autorizzazioni sia quello di assegnare i permessi di accesso alle risorse in base al ruolo ricoperto dall’utente all’interno dell’organizzazione; pertanto, il passaggio ad una gestione delle policy basata su ruoli funzionali, diventa l’elemento fondamentale di questa fase progettuale. In questa fase si inserisce il tema del Compliance Management, che si propone la verifica del modello profilativo individuato prima ancora della sua realizzazione.

USER PROVISIONING E WORKFLOW. L’insieme delle operazioni di amministrazione che portano alla definizione degli account utente e all’attribuzione dei diritti di accesso

in base al ruolo, prende il nome di User Provisioning; una soluzione efficiente di IAM introduce un sistema di gestione centralizzata di tutto il processo di amministrazione. A supporto di tale strumento si pone la componente di Workflow, che permette di automatizzare il processo di provisioning inviando ai relativi sistemi, o anche a persone fisiche, le notifiche necessarie al completamento dell'intero processo.

AUTENTICAZIONE UTENTI. L'autenticazione è il processo che verifica l'identità di un utente in modo da poter correttamente permettere o negare l'accesso a risorse condivise e protette. Le tecniche di autenticazione possono spaziare dal semplice login con username e password a meccanismi più complessi e forti come token, certificati digitali a chiave pubblica e sistemi biometrici.

Una soluzione di IAM deve pertanto essere indipendente dal meccanismo di autenticazione utilizzato in modo da potersi adattare ad ogni specifica realtà tecnologica. Inoltre, in una organizzazione che rispecchi lo scenario descritto inizialmente, l'utente si trova spesso ad accedere a numerose applicazioni, siano esse web-based o client-server, comportando l'impiego di numerose credenziali differenti. Per questi motivi, un altro tassello chiave di una efficiente strategia di IAM è costituito dall'implementazione di una soluzione di Single Sign On: questa permette da un lato di semplificare il lavoro degli utenti e dall'altro di diminuire il carico amministrativo del personale IT ed il supporto dell'Help Desk.

Per quanto sopra detto, in relazione alle risorse, ai tempi ed ai costi necessari per realizzare ad una soluzione di IAM, vale la pena sottolineare come questa possa essere sviluppata, nel suo complesso, in fasi differenti; la strategia di implementazione deve basarsi sempre sulle priorità di business dell'organizzazione partendo, tra le macro attività sopra elencate, da quella prioritaria per l'azienda; si riportano di seguito alcuni esempi:

- l'introduzione di una nuova applicazione da distribuire ad un grande numero di utenti (con relative credenziali di autenticazione) sposta necessariamente l'attenzione su una soluzione di user provisioning che permetta una più efficiente gestione dei processi amministrativi;
- un'organizzazione principalmente orientata ad attività di e-business può portare l'introduzione di una soluzione di IAM da un punto di vista più applicativo che organizzativo;
- la necessità di ridurre la complessità di lavoro degli utenti, legata a numerose credenziali di accesso alle diverse applicazioni, conduce a porre l'attenzione principalmente su una soluzione di Single Sign On.

IL VALORE REPLY

Il successo di una soluzione di IAM non risiede nel solo coinvolgimento del personale IT, ma dipende dal supporto e dall'impegno di tutta l'organizzazione aziendale.

Spike Reply, avvalendosi anche della competenza diffusa all'interno del Gruppo Reply, realizza progetti di Identity and Access Management sfruttando una metodologia proprietaria in grado di adattarsi alle specifiche esigenze del Cliente e verificata con il best of breed delle soluzioni tecniche disponibili sul mercato. Si pone quindi come interlocutore preparato sia dal punto di vista tecnologico, nella scelta della soluzione che meglio si adatti al business principale del cliente, sia dal punto di vista organizzativo, nell'analisi della metodologia di approccio alle tematiche dell'Identity and Access Management e nella revisione dei processi organizzativi che ne derivano.

Le principali referenze sulla tematica IAM vedono Reply impegnata su realtà complesse dei mondi Finance e Industry in progetti di ambito internazionale.

Partendo da una competenza consolidata sul campo da molteplici esperienze, dalla conoscenza approfondita delle tecnologie, degli operatori, degli standard di riferimento e delle leggi e operando poi una costante verifica delle contromisure adottate, delle procedure operative ed organizzative, della configurazione dei sistemi, delle applicazioni e delle reti, Spike Reply è in grado di aiutare i Clienti a costruire lo "scudo" più efficiente contro qualsiasi tipo di minaccia e di fornire la massima garanzia su tutte le fasi di intervento.

Nello specifico, Spike Reply è in grado di fornire:

Consulenza (Piano della Sicurezza, Analisi e Gestione del Rischio, Adempimenti Legislativi, Policy e Procedure, Verifica della Sicurezza del Sistema Informativo, Security Consolidation)

Progettazione Soluzioni ICT (Studi di fattibilità, Project assessment, Software selection, Project selection)

Realizzazione Soluzioni ICT (Soluzioni chiavi in mano, Gestione e Manutenzione, Presidio, Help Desk, Test)

Formazione (Security Awareness aziendale, Formazione ICT)

Nello svolgimento delle proprie attività Spike Reply si avvale di tutte le risorse condivise a livello di Gruppo Reply e delle relazioni sviluppate con un network di società partner che forniscono principalmente prodotti tecnologici o servizi di consulenza.



All'interno del Gruppo Reply SpA, Spike Reply è la società specializzata sulle tematiche relative all'area della Sicurezza e della tutela dei Dati Personali.

Spike Reply ha definito un'offerta completa, integrata e coerente per affrontare ogni aspetto del rischio associato ad un sistema informativo: dall'individuazione delle minacce e delle vulnerabilità, alla definizione, progettazione e di implementazione delle relative contromisure tecnologiche, legali, organizzative, assicurative o di ritenzione del rischio.

La missione di Spike Reply è di permettere ai propri clienti di effettuare il loro business in condizioni di Sicurezza, supportandoli nello sviluppo delle idonee strategie e nella implementazione delle appropriate soluzioni per una gestione efficace della Sicurezza delle Informazioni.

Spike Reply
www.reply.eu