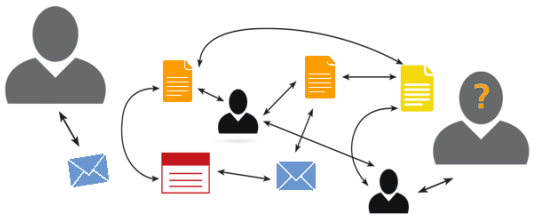
ELD Access Management

In un ambiente aziendale strutturato e di una certa complessità sorge spesso il bisogno di gestire le richieste da parte degli utenti che hanno l'esigenza di accedere a determinate risorse od applicativi aziendali.

Se in molti casi queste richieste di autorizzazione vengono veicolate via email o tramite le procedure aziendali di Incident management è anche vero che un processo strutturato, creato appositamente e focalizzato a questo tipo di gestione aiuta l'azienda a tenere sotto controllo il processo , le autorizzazioni rilasciate e quindi il livello di sicurezza dei sistemi.

Controllare chi e come richiede di accedere alle informazioni ed i dati (nonché alle applicazioni) di natura riservata rende intrinsecamente più sicuri i sistemi aziendali, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità), sia dalla possibilità che un utente non autorizzato possa modificarli (integrità).



"La gestione dell'identità e dell'accesso (IAM) è la disciplina di sicurezza che consente agli individui giusti di accedere alle risorse giuste nei momenti giusti per ragioni giuste. Questa pratica di sicurezza è un'impresa cruciale per qualsiasi impresa." - Gartner

Inoltre la possibilità di generare report della situazione in qualunque momento permette di verificare lo stato delle autorizzazioni, rispondendo ad esempio alle richieste dell'audit o della direzione interna e permettendo di apportare azioni corretive mirate nel caso in cui la sensibilità delle informazioni sia cambiata.

Eld Access Management (**ELD-AM**) è un pacchetto software dedicato alle aziende che permette di gestire le anagrafiche utenti e le relative richieste di autorizzazioni all'interno di un sistema informativo più o meno complesso. In questa versione è disegnato per funzionare all'interno del client Notes mentre è già previsto a breve il rilascio con interfaccia browser.

In particolare i principali obiettivi di ELD-AM sono:

- la realizzazione di un'anagrafica aziendale del personale (dipendenti,stagisti, distaccati) ed eventualmente di persone esterne
- presidiare e controllare la corretta assegnazione delle abilitazioni software e delle dotazioni hardware garantendone il monitoraggio ed un processo strutturato e puntuale per l'attribuzione delle stesse
- definire la responsabilità delle risorse (applicazioni e/o dati)
- garantire trasparenza e tracciabilità delle richieste
- gestione di Workflow e processi di approvazione delle richieste
- rendere disponibili in ogni momento report sulla situazione , specialmente ad uso dell'IT , dell'audit aziendale o per verificarne la compliance
- verificare il catalogo delle applicazioni/risorse aziendali per cui è possibile richiedere accesso
- verificare i livelli di accesso disponibili per ogni applicazione/risorsa
- aumentare la facilità d'uso del sistema informativo da parte degli utenti finali
- supporto per compliance alla normativa, in particolare PCI e GDPR

ELD-AM gestisce due tipi principali di documenti : le persone e le risorse.

Per **risorse** si intendono tutte quelle entità/funzionalità per cui è possibile chiedere (o revocare) un' autorizzazione come, ad esempio, dischi condivisi di rete, accessi a database o ad applicativi. All'interno di ELD-AM ne viene gestito il catalogo completo al cui interno ogni risorsa ha una serie di caratteristiche.

A loro volta le risorse sono suddivise in categorie per permetterne una più rapida localizzazione . Per ogni risorsa è possibile definire una serie di caratteristiche quali i livelli di accesso previsti (lettura, lettura e scrittura ecc.) il proprietario della risorsa e la sensibilità della risorsa stessa.

Questa informazione introduce il concetto di sensibilità (normale, media od alta) della risorsa stesssa . Nel caso siano medie od alte per la risorsa viene definito un proprietario che sarà notificato in caso di nuova richiesta di accesso e che, a seconda della sensibilità, dovrà dare esplicita autorizzazione all'accesso.

La gestione delle **persone** invece permetterà, oltre ad avere una anagrafica aziendale completa, di notificare gli interessati dell'arrivo di una nuova persona in azienda . In questo modo è possibile preparare in anticipo le dotazioni , le utenze e gli accessi per il nuovo arrivato.

Al contrario diviene più semplice la gestione della persona che lascia l'azienda in quanto , tramite apposita funzione, vengono generate le notifiche di disabilitazione per tutto quanto in essere.

Inoltre viene gestito anche il caso del "cambio incarico" cioè della persona che, all'interno dell'azienda, cambia mansioni e responsabilità. Senza una gestione di questa casistica capita che tale persona mantenga le abilitazioni precedenti accumulandole a quelle necessarie al nuovo incarico , spesso senza reale bisogno o peggio ancora in contrasto col nuovo incarico.

Sempre più attacchi (e minacce latenti) arriveranno dall'interno. I dipendenti sono spesso la fonte degli attacchi più pericolosi.

Queste minacce sono più difficili da identificare, perché i dipendenti utilizzano credenziali utenti legittimate. Possono provocare gravi danni visto che hanno un accesso privilegiato alle informazioni necessarie per il loro lavoro e possono accedere ad una grande varietà di dati.

Infatti i dipendenti, anche quando non sono animati da cattive intenzioni, potrebbero veicolare vulnerabilità (tramite device Usb o file scaricati dalla rete) tanto quanto dei sabotatori intenzionali.

Le organizzazioni hanno bisogno di combattere queste minacce dall'interno avendo maggiore visibilità e controllo sui propri sistemi interni, oltre che cercare di rafforzare il perimetro della rete.

Avere sotto controllo e poter verificare lo stato delle abilitazioni è un passo importante, così come è fondamentale non avere persone con abilitazioni non necessarie .

Il Request Fulfilment in ITIL v3

Il processo di Request Fulfilment e' nuovo con ITIL v3. Questo processo e' parte del Service Operation nell'ambito del lifecycle in ITIL v3. Gli obiettivi di questo processo sono i seguenti:

- Fornire agli utenti un canale per richiedere (e ricevere) servizi standard per i quali esiste uno schema predefinito di approvazione (i.e. richiesta di un computer)
- Fornire agli utenti informazioni sui servizi disponibili e sulle procedure per ottenerli
- Fornire i servizi standard di cui sopra agli utenti finali

Per ogni tipologia di Service Request fovrebbe esserci un chiaro flusso di attivita' che determini la fornitura (o non approvazione) del particolare servizio all'utente.