LE POLITICHE DI ACCESSO: LA POLITICA DI ACCESSO DISCREZIONALE

Si può rappresentare facilmente mediante la matrice degli accessi.

Il proprietario della risorsa può in ogni momento e a proprio piacimento modificare i diritti di accesso degli altri utenti modificando l'opportuna casella della matrice. Questa discrezionalità è allo stesso tempo una forza della politica, perché la rende semplice ed estremamente flessibile, ma anche una forte debolezza, proprio perché manca un controllo generale e tutto è lasciato alla decisione del possessore della risorsa.

MANDATORY ACCESS CONTROL

Un altro tipo di politica di controllo degli accessi è il MAC (Mandatory Access Control). Il MAC consiste nell' assegnare ad ogni utente un "grado" e ad ogni risorsa un livello di sicurezza. L'accesso viene consentito se e solo se il "grado" dell'utente è adeguato al livello di sicurezza della risorsa.
Chi ha l'autorizzazione per accedere a una risorsa non può, solo di sua spontanea volontà, consentire a un'altra entità di accedere a quella risorsa. E' un sistema sicuro ma poco flessibile.

ROLE-BASED ACCESS CONTROL

I diritti di accesso vengono assegnati sulla base dei ruoli piuttosto che sugli utenti direttamente. Agli utenti vengono assegnati ruoli staticamente o dinamicamente secondo le loro responsabilità nel sistema. Ad ogni ruolo corrisponde il diritto di accesso ad alcune risorse.
La relazione tra utenti e ruoli è molti a molti RBAC sta diventando sempre più popolare grazie al suo alto grado di flessibilità

ATTRIBUTE-BASED ACCESS CONTROL

L'attribute-based access control **(ABAC)** è un nuovo approccio che sta riscuotendo sempre più consenso grazie alla sua flessibilità.
Consiste nel stabilire i diritti di accesso in base ad attributi e caratteristiche della risorsa, dell'utente (organizzazione, titolo, area di lavoro) e anche di circostanze esterne (data, livello di sicurezza della rete). ABAB implementa una regola che prende in ingresso questi attributi e restituisce il responso come output.

RIFERIMENTI

- https://www.c3t.it/projects/awareness/articoli&brochure/controllo_accessi/

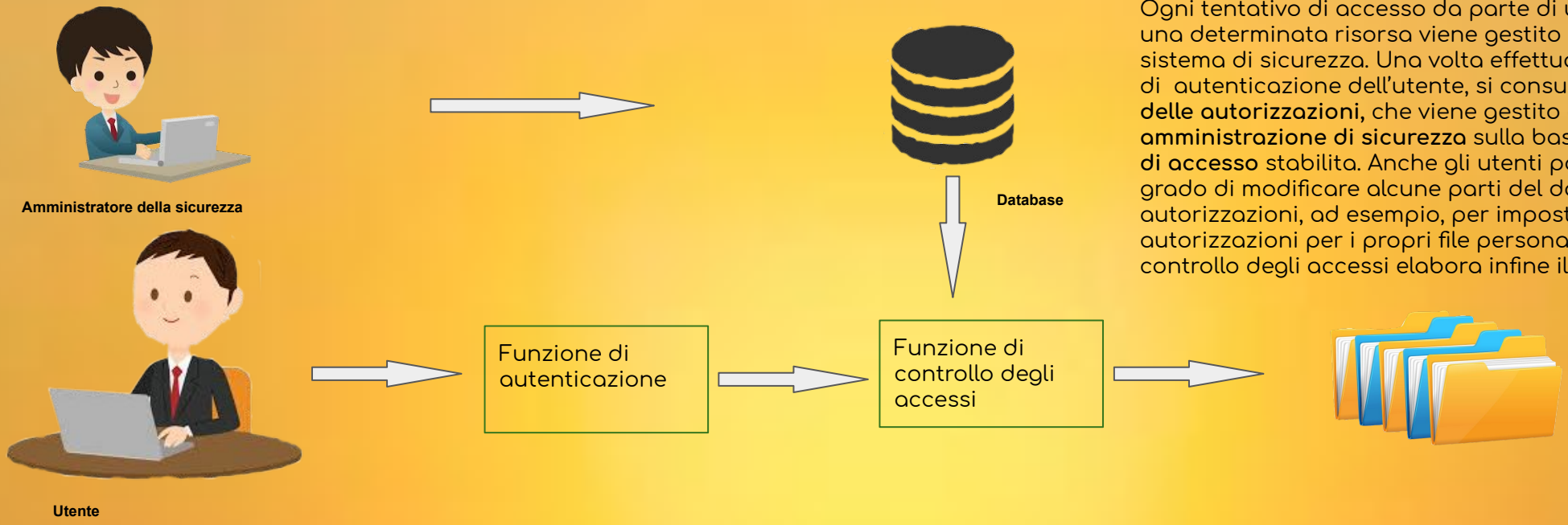
POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

IL CONTROLLO DEGLI ACCESSI

Scopri perchè è importante e come può essere implementato

IL PROBLEMA DEL CONTROLLO DEGLI ACCESSI

Conoscere l'identità di un individuo che richiede l'accesso ad un sistema (autenticazione) non è abbastanza per avere un sistema completamente sicuro. In sistemi particolarmente complessi infatti, con centinaia o migliaia di utenti e un gran numero di risorse o servizi, il problema di stabilire chi ha accesso a cosa non è affatto banale.
Lo scopo del **controllo degli accessi** consiste nel limitare le azioni o operazioni che utenti o programmi di un sistema informatico possono eseguire all'interno di un sistema complesso, in modo da prevenire violazioni e rischi per la sicurezza dell'intero sistema.
NISTIR 7298 definisce il controllo degli accessi come il processo di concedere o negare specifiche richieste per:
- ottenere e utilizzare le informazioni e le relative informazioni servizi di elaborazione
- accedere a strutture fisiche specifiche



Ogni tentativo di accesso da parte di un utente ad una determinata risorsa viene gestito e vagliato da un sistema di sicurezza. Una volta effettuato il processo di autenticazione dell'utente, si consulta il **database delle autorizzazioni,** che viene gestito dalla **amministrazione di sicurezza** sulla base della **politica di accesso** stabilita. Anche gli utenti possono essere in grado di modificare alcune parti del database delle autorizzazioni, ad esempio, per impostare le autorizzazioni per i propri file personali. La funzione di controllo degli accessi elabora infine il responso finale.

Ogni sistema di controllo degli accessi ben progettato viene accoppiato con l'**auditing**. I controlli di auditing riguardano l'analisi a posteriori di tutte le richieste e attività degli utenti nel sistema. L'auditing richiede la registrazione di tutte le richieste degli utenti e delle attività per la loro successiva analisi. I controlli di auditing sono utili sia come deterrenti per scoraggiare gli utenti dal tentare violazioni, dal momento che sanno che tutte le loro richieste vengono monitorate, ma anche come mezzo per analizzare il comportamento degli utenti durante l'utilizzo del sistema per scoprire possibili tentativi di violazione o violazioni effettive.

Nel controllo degli accessi bisogna fare un distinzione tra **politiche di accesso** e **meccanismi di accesso.**
Le politiche sono linee guide di alto livello che determinano come i controlli sugli accessi vengono effettuati e come la decisione se consentire o negare gli accessi viene presa.
I meccanismi di accesso sono invece software o hardware di basso livello che vengono implementati per eseguire la politica.
I controlli di auditing riguardano l'analisi a posteriori di tutte le richieste e attività degli utenti del sistema. L'auditing richiede la registrazione di tutte le richieste degli utenti e delle attività per la loro successiva analisi.