Администриране на достъп до информационни системи: основни понятия, технологии, сигурност

При управлението на достъпа в информационните системи преди всичко се контролира идентифицирането на легалните потребители, проверява се тяхната легалност и правата им.

Преди обръщане към информационната система потребителят трябва да съобщи на системата за управление на базата данни своя идентификатор, обикновено съпровождан от парола. Определянето на идентификаторите и паролите на потребителите е административна работа и от нейната секретност зависи защитата на информационната система. Проверката и потвърждаването на коректността на идентификатора и паролата се основава на изпълнението на специална процедура. В някои системи за проверка на потребителите се използват магнитни или смарт-карти, каталогизиране на биометрични данни. Самата проверка на привилегиите може да се извърши на различни нива. Проверката на правата на достъп може да се извърши по време на компилацията без достъп до информацията в системата. Достъпът до определена част от информационната система може да се проверява при отваряне на файл с данни или при всяка транзакция, която се обръща към системата.

Изборът на стратегия за защита се извършва от ръководството на концептуално ниво при проектирането на информационните системи. На този етап трябва да се решат проблемите за ограничаване на достъпа и да се избере тип на системата. За ограничаването на достъпа съществуват два основни метода: 1. Метод на минималната привилегия („need-to-know“ policy). Съгласно този метод субектите в системата използват минимално количество информация, нужно само за тяхната дейност. 2.Метод на максималната привилегия („maximum availability“), основан на принципа за максимална достъпност. Този метод е подходящ при изграждане на информационни системи за университети или изследователски центрове, които не се нуждаят от секретност.

За повечето потребители традиционните системи за управление на достъпа са много сложни за администриране. Броят връзки е пропорционален на произведението на броя потребители по броя обекти. Необходими са решения в обектноориентиран стил, които да намалят тази сложност.Такова решение е управлението на достъпа чрез роли. Същността му е в това. че между потребителите и правата им се появяват междинни звена-роли. За всеки потребител могат да бъдат едновременно активни няколко роли, всяка от които му дава определени права. Достъпът чрез роли е неутрален по отношение на конкретните видове права и начините за проверката им. Чрез този метод може да се управлява подсистемата за разграничаване на достъпа даже и при голям брой потребители. Управлението на достъпа чрез роли е свързано със следните основни понятия:**потребител** (човек, интелектуален автономен агент и т.н.);**сеанс** на работата на потребителя; **роля** (обикновено се определя в съответствие с организационната структура); **обект** (достъпът до него се разграничава, напр., файл на операционната система или таблица от СУБД); **операция** (зависи от обекта; напр. за файлове на операционните системи - четене, запис, изпълнение и т.н., за таблици от СУБД - добавяне, изтриване и т.н.); **право на достъп** (разрешение да се изпълняват определени операции върху определени обекти).