50. Сигурност на информационни системи – софтуерни технологии и решения

Мрежовата сигурност има за цел да предпази мрежово достъпните ресурси на информационната система от неоторизиран достъп, злоупотреба, модификация или предизвикване на отказ на услугата. Включва оторизация на достъп до данни в мрежата. Потребителите използват или имат предписано ID (идентификация) и парола, или друг тип автентизираща информация, която им позволява достъп към информация или програми. Мрежовата сигурност обикновено започва с автентикация на потребителя най-често чрез потребителско име (username) и парола (password). Автентикацията е еднофакторна, когато се осъществява чрез парола, която потребителят знае, двуфакторна, когато се използва допълнителен достъп. Съществува и трифакторна автентикация (напр. чрез биометрични данни - пръстов отпечатък).

Към методите за осигуряване на мрежова сигурност са включени: витуална частна мрежа, система за засичане на проникване (Intrusion detection system – IDS), PKI (Public Key Infrastructure) , електронен подпис, Firewall. Електронният подпис е реквизит на електронен документ, предназначен за защитата му от фалшификация. Издава се от сертифициращ орган и съдържа името на титуляра, сериен номер, дата на валидност и копие от публичния ключ. Firewall (защитна стена) е система, проектирана да контролира преминаването на информация от една мрежа във втора мрежа. Защитната стена определя кои вътрешни услуги могат да са достъпни отвън и обратно. Най-често защитните стени работят на нивото на мрежовия и транспортния слой, където изследват пакетите данни на TCP/IP протоколите и взимат решенията си в зависимост от IP адреса на изпращача и други параметри. Съществуват три основни вида защитни стени – филтриращи маршрутизатори (filtering routers), поддържащи връзката пакетни филтри (stateful packet filters) и приложни шлюзове (application gateways).

Антивирусен софтуер е сборното название на всички видове софтуерни приложения, предназначени за предпазване от и отстраняване на компютърни вируси и други злонамерени програми при персоналните компютри. Задачата на антивирусния софтуер е да предпазва компютъра, като постоянно следи файловете, които се изпълняват и отварят за възможни заплахи.

Автентикацията при съвременните системи за управление на бази данни най-често е еднофакторна, т.е. използва се потребителско име и парола. SQL-базираните СУБД предлагат шест нива на на достъп (SELECT, INSERT, UPDATE, DELETE, REFERENCES, ALL PRIVILEGES), като това прави възможно създаването на потребители с различни нива на достъп. Mirroring на бази данни е предимно софтуерно решение за увеличаване на достъпността на базите данни. Когато mirroring сесията на базата данни е синхронизирана, се предоставя резервен сървър, който е способен да се възстанови бързо след срив без да загуби данни от изпълнените транзакции. За сигурността на базите данни са неизбежни резервните копия (backup) и плановете за възстановяване (recovery plans).