SIGURNOSNI SERVISI

U računarskim mrežama se u cilju sprečavanja eventualnih napada na mrežu i mogućih oštećenja podataka realizuju sledeći sigurnosni servisi:

- autentifikacija (engl. authentication),
- tajnost podataka (engl. data confidentiality),
- neporicanje poruka (engl. nonrepudation),
- integritet podataka (engl. data integrity),
- kontrola pristupa (engl. access control),
- raspoloživost resursa (engl. resource availability).

Autentifikacijom se dokazuje identitet korisnika i sistema koji šalje poruku. Pored toga autentifikacija treba da spreči mogućnost lažnog predstavljanja i neautorizovanu fabrikaciju poruka u mreži. Realizuje se uz pomoć različitih kriptografskih tehnika: šifrovanja, digitalnih potpisa, vremenskih pečata i sl.

Tajnost podataka obuhvata zaštitu podataka od presretanja od strane neovlašćenog lica. Realizuje se fizičkom zaštitom komunikacionog medija i kontrolom pristupa.

Da bi se sprečila pojava da primalac po volji izmeni primljenu poruku a da zatim tvrdi da ju je upravu kao takvu i primio, primenjuje se servis neporicanja poruka. Mehanizam koji obezbeđuje ovaj sigurnosi servis je digitalni potpis.

Servis integriteta podataka obezbeđuje integritet i tačnost poruke koja se prenosi, odnosno, sprečava mogućnost promene tela i zaglavlja poruke bez obzira da li je promena rezultat namernog ili nenamernog oštećenja. Kontrola pristupa obezbeđuje regulisanje odnosa između korisnika i resursa mreže. Najbezbednije rešenje je svakako fizičko odvajanje pojedinih segmenata ili celokupne mreže odnosno sprečavanje svakog pristupa računarskoj mreži. Sa druge strane moguće je vršiti filtraciju mrežne komunikacije i na taj način omogućiti restriktivan pristup ili zabranu pojedinim komunikacionim servisima. Filtraciju vrše posebni komunikacioni serveri koji se obično nazivaju mrežnim barijerama (engl. firewalls).

Raspoloživost resursa označava servise koji imaju za cilj održavanje funkcionalnosti računarskih mreža u slučaju otkaza mrežne opreme ili napada na mrežu.

U SAD postoje standardi koji definišu potreban nivo sigurnosnih servisa u računarskim mrežama a koji su objedinjeni u takozvanoj crvenoj knjizi (engl. red book). Pun naziv ove knjige je Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria i ona u stvari predstavlja nadograđenje već postojeće narandžaste knjige (engl. orange book) koja se odnosila na sigurnost izolovanih računara.