Zaštita i sigurnost informacijskih sustava

Vrsta: Seminarski | Broj strana: 13 | Nivo: FER

Sadržaj

Uvod 2
1. Osnove informacijske sigurnosti 3
1.1. Zaštita informacijskih sustava 4
1.2. Norma ISO/IEC 17799:2000 5
2. Opseg Europske politike 8
3. Zakonski okvir u RH 10
Zaključak 12
Literatura 13

Uvod

Poznavanjem informacija čovjek postaje uspješniji u svom radu i kreativnom stvaranju, sprječava nezgode, loša rješenja i odluke, neutralizira greške, smanjuje utjecaj nepredviđenih situacija. Pravodobna informacija u današnjem svijetu predstavlja pravo zlato, pogotovo u financijskom svijetu. Informacija postaje sredstvo trgovanja. Naravno, kako informacija ima neku vrijednost, ona postaje metom krađa, zloupotrebe, diskreditacije. Kao što nas povijest uči, informacije se moraju čuvati te pohranjivati za buduće naraštaje.

Sigurnost informacija u nekom sustavu je realnost i potreba. Izgradnja upravljivog sustava sigurnosti je nužnost u poslovnom svijetu, ali sve više i u ostalim organizacijama.

U današnje vrijeme uspostava sigurnog informacijskog sustava je prepoznata kao potreba pa se razvijaju brojni standardi koji uključuju najbolju praksu i preporuke o upravljanju sigurnosti informacijama.

Da bi se uspješno zaštitili informacijski sustavi, donesen je veliki broj zakona i pravnih normi koji imaju za cilj da pospješe sigurnost informacijskih sustava.

Upravo o sigurnosti informacionih sistema i načinima zaštite istih govoriti ćemo u ovom seminarskom radu.

1. Osnove informacijske sigurnosti

Informacijska sigurnost definira se kao sposobnost obrane informacijskog sustava od gubitka dostupnosti, narušavanja integriteta i kompromitiranja tajnosti informacija koje su spremljene ili koje se prenose uporabom određenih servisa, a koji mogu biti ugroženi nenamjernim događajima ili malicioznim akcijama.

Informacijska sigurnost ima glavne ciljeve, a to su :

zaštita informacija koje se razmjenjuju putem mreža i informacijskih sustava od narušavanja integriteta i gubitka dostupnosti,

zaštita informacija od sabotaže i malicioznih akcija,

ograničavanje posljedica i usvajanje potrebnih dopunskih mjera u slučaju ugrožavanja (napada).

Osnovi principi sigurnosnih mjera su :

osigurati dostupnost, integritet i tajnost informacija,

osigurati da se informacijama pristupa na temelju načela „need-to-know“,

spriječiti bilo kakvu vrstu neovlaštenog pristupa klasificiranim informacijama,

osigurati identifikaciju osoba čiji položaj može ugroziti sigurnost klasificiranih informacija.

Potpuna (apsolutna) informacijska sigurnost ne postoji! U većini slučajeva „apsolutna“ zaštita dovodi do toga da je ugrožavanje u bilo kojem obliku (vremenskom, financijskom, ljudskom, sigurnosnom itd.) apsolutno neisplativo. Međutim, odsustvo minimalno potrebne zaštite spada u domenu maksimalno mogućeg ugrožavanja rada pojedinca i organizacije. Pri tome je kvaliteta, osiguranje kvalitete i upravljanje kvalitetom bilo koje i bilo kakve organizacije fiktivna kategorija.

Sigurnost informacijskih sustava unutar EU poznata je pod nazivom INFOSEC i ona podrazumijeva nekoliko ostalih tipova sigurnosti :

sigurnost podataka na elektroničkim medijima i računalima (COMPUSEC),

sigurnost podataka u sustavima za prijenos podataka (COMSEC),
sigurnost informacijske infrastrukture u posebnim kategorijama prostora od različitih vrsta prisluškivanja (TECSEC).