SIGURNOST INFORMACIJSKIH SUSTAVA

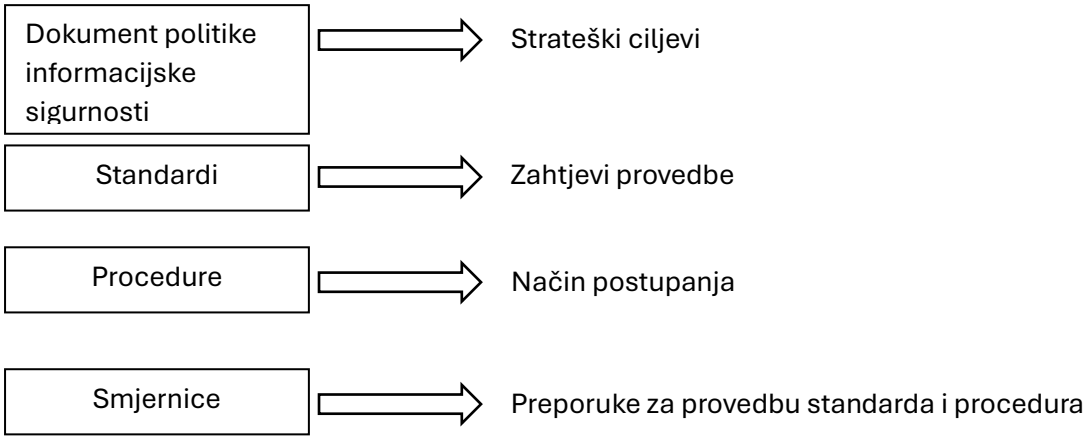
(S-I-S)

Koncept informacijske sigurnosti

Informacijska sigurnost – dio sigurnosti koja ima dokumente kojima se utvrđuju mjere i standardi informacijskih sustava.

Ne odnosi se isključivo o podacima koji su pohranjeni na računalu.

Sve informacije koje je potrebno zaštiti od neovlaštenog pristupa, promjene ili uništavanje bez obzira na oblik i mjesto gdje su informacije pohranjene.



Zakoni vezani za RH

Zakon o sigurnosno-obavještajnom centru

Zakon o informacijskoj sigurnosti

Zakon o tajnosti podataka

Zakon o zaštiti podataka

ISO 27000 standard – smjernica svim tvrtkama koje žele uvesti sustav upravljanja informacijskih sustava.

6 standarda od kojih je ISO27001 središnji standard, nema uputa za implementaciju nego kontrole koje treba provoditi.

ISO27001 se koristi npr. za bankovne sustave.

LV01 – Zakonska regulativa IS

1.
    a) Što je informacijski sustav?

IS je sustav koji prikuplja, pohranjuje , čuva, obrađuje i isporučuje potrebne informacije uz nekakvu autorizaciju.

    b) Što su mjere informacijske sigurnosti?

Mjere informacijske sigurnosti su opća pravila zaštite podataka koje se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.

    c) Što je osobni podatak?

Osobni podatak je podatak koji se odnosi na pojedinca.

    d) Koje osobne podatke je zabranjeno prikupljati?

Podatci o rasi, etničkom podrijetlu, političkim stajalištima, vjeri, o kaznenom/prekršajnom postupku i sl.

    e) Što je klasificirani, a što neklasificirani podatak?

Klasificirani podatak je podatak koji ima važnost povjerljivosti te ima stupanj tajnosti, a neklasificirani nema stupanj tajnosti.

    f) Što je deklasifikacija?

To je postupak kojim se utvrđuje prestanak postojanja razloga zbog kojih je određeni podatak klasificiran.

    g) Što je CERT?

Organizacijski entitet koji reagira na računalno-sigurnosne incidente.

    h) Što je certifikat?

Potvrda.

    i) Stupnjevi klasifikacije podataka

VRLO TAJNO, TAJNO, POVJERLJIVO, OGRANIČENO.

    j) Što je PCI-DSS?

To je globalni standard za zaštitu podataka o plaćanju karticama.

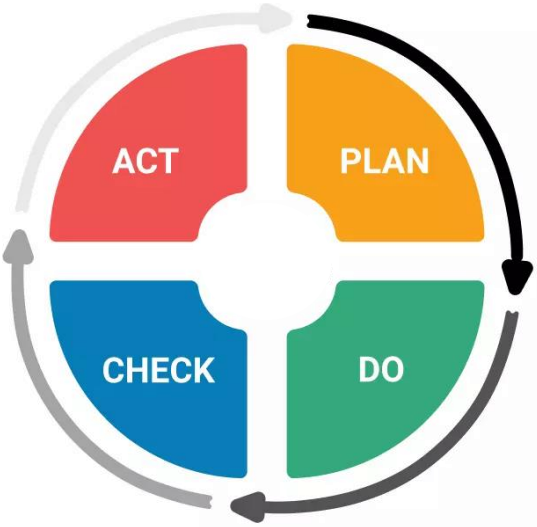
    k) 5 sigurnosnih zahtjeva PCI-DSS-a.

Zaštiti kartične podatke, testirati sig. sustave , održavati politiku IS,razvijati sigurne sustave, ograničiti fizički pristup.

l) Što opisuje PDCA model sigurnosti?

Omogućava organizacijama da poboljšaju sigurnosne prakse kroz proces čime se povećava učinkovitost.

PDCA ciklus (ISO-27001)



Planiranje – sve aktivnosti unaprijed planirati

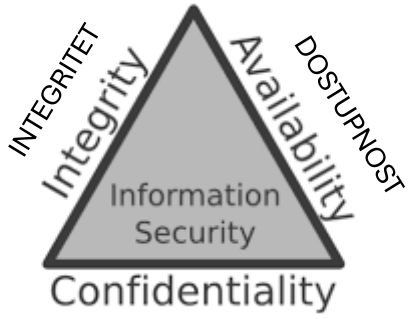
Implementacija – faza implementacije planiranih aktivnosti

Provjera – mjerenje i nadzor implementiranih kontrola

Djelovanje – ovježavanje procesa u svrhu unaprijeđenja

CIA TROKUT

Model sigurnosti informacijskog sutava kao zbroj 3 ključne komponente



POVJERLJIVOST

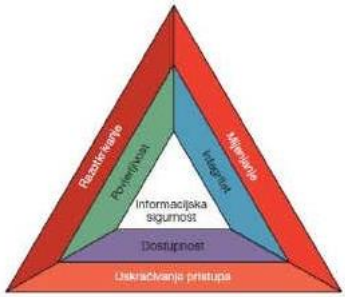
Povjerljivost zahtjeva da samo one osobe koje trebaju imati pristup taj pristup i imaju.

Integritet osigurava da samo ovlaštene osobe mogu promijeniti pohranjene informacije.

Dostupnost omogućava autoriziranim korisnicima stalan pristup.

DAD trokut

Predstavlja 3 napada na 3 osnovne komponente CIA trokuta.



Osnovna terminologija ISO27000 standarda

Sigurnosna ranjivost predstavlja grešku ili nedostatak u bilo kojem elementu informacijskog sustava.

Tri grupe :

- Prirodne prijetnje (potresi,poplave...)
- Ljudske prijetnje (najčešće u vidu neovlaštenih korisnika)
    - Napadač pokušava narušiti jednu/više komponenti CIA trokuta
- Prijetnje okoline (ispadi el. energije, zagađenja...)

Exploit – specijalna kategorija programa, grupe podataka ili naredbi koje u tom obliku iskorištavaju sigurnosnu ranjivost.

Sigurnosni rizik – predstavlja mogućnost ostvarivanja prijetnje, odnosno štete.

Računa se : R = F(AV, V , T, P , I)

Pri čemu su : vrijednost resursa (AV)

Ranjivost resursa (V)

Prijetnje koje mogu iskoristiti ranjivosti (T)

Vjerojatnost ostvarivanja (P)

Posljedice (I)

Višeslojni strateški model sigurnosti

Model zaštite informacijskog sustava od bilo kojih zabranjenih aktivnosti pomoću višestrukih razina zaštite.

Podatkovna razina

Podatke na ovoj razini štitimo postavljanjem prava pristupa te enkripcijom i korištenjem zaporki.

Aplikacijska razina

Obuhvaća sve aplikacije, odnosne servise čije sigurnosne ranjivosti napadači pokušavaju iskoristiti.

Računalna razina

Obuhvaća računala odnosno poslužitelje na kojima su pokrenute aplikacije i podaci.

Vanjska granica RM (perimeter)

Točka kontrole i razdvajanja interne mreže i javne mreže.

Fizička razina

Kontrolira fizički pristup RM i poslužiteljima.

Definiraju se metode zaštite.

Fizički sloj

Fizička sigurnost poslužitelja predstavlja velik izazov za tvrtku.

Napadač koji ima pristup poslužitelju može pokrenuti niz napada koji je težak spriječiti.

Ne štiti stopostotno.

Odvraćanje napadača – ispravno postavljene sigurnosne kontrole.

Otežavanje napada – uspostavljanje višestrukih sigurnosnih mehanizama.

Omogućavanje detekcije napada – sigurnosne kontrole poput videonadzora.

Građevina i okoliš

Mehanizmi fizičke zaštite

Potrebno posvetiti pažnju samim građevinama u kojima će biti postavljene sistemske sale, ali prostorijama gdje će zaposleni raditi.

Potrebno je planirati raspored i upotrebu prostorija.

Pri procjeni i odabiru lokacije bitno je:

- Infrastruktura u vidu napajanja sustava.
- Mogući opasni materijali u okolini građevine.

Ograde do 1,2/1,8/2,4m visine.

Ograničavanje pristupa

Pažnju posvetiti izradi vrata, odn. zonama pristupa kojima pojedini zaposlenici smiju pristupiti.

Beskontaktne kartice.

Podijeliti zgradu na zone za zaposlene i posjetitelje.