Javno/Public
SCC d.o.o. Beograd

SCC

SCC d.o.o.
Br: 536/2022
Datum: 05.08. 2022 god.
Beograd

Inženjerski principi bezbednosti informacija

Budući da bezbednost informacija mora biti obuhvaćena u upravljanju projektima, bez obzira na vrstu projekta, i da mora biti osmišljena i ostvarena tokom životnog veka razvoja sistema, u SCC d.o.o. Beograd se primenjuju sledeći inženjerski principi bezbednosti informacija:

1. U SCC d.o.o. Beograd su ustrojene čvrste i jasne politike bezbednosti informacija kao temelj za razvoj i primenu informaciono-komunikacionih tehnologija (IT).
2. Bezbednost informacija se posmatra kao sastavni deo ukupnog sistema razvoja i primene IT.
3. Jasno je ocrtana granica između fizičke i logičke bezbednosti rukovodeći se odgovarajućim skupom politika bezbednosti informacija.
4. Smanjuju se rizici na prihvatljiv nivo.
5. Svi spoljni sistemi se posmatraju kao nebezbedni.
6. Prihvaćeno je stanovište da smanjenje rizika košta, kao i da obara radne sposobnosti i neke funkcionalnosti IT sistema.
7. Primenjuje se slojevita bezbednost (sa više nivoa).
8. Uvedene su prilagođene mere bezbednosti koje idu u susret ciljevima SCC d.o.o. Beograd.
9. Teži se najvećoj mogućoj jednostavnosti.
10. Projektuje se i koristi onakav IT sistem koji ograničava ranjivosti i prilagodljiv je u odgovoru.
11. Bezbednost se uvodi primenom usklađenih fizičkih i logičkih mera zaštite.
12. Osigurava se da sistemi mogu da rade neprekidno i da su prilagodljivi u susretu sa različitim pretnjama.
13. Ograničene su i lokalizovane ranjivosti.
14. Oblikovane su mere bezbednosti koje pokrivaju što širi opseg za zaštitu.
15. Izolovani su javno dostupni sistemi od sopstvenih životnih sredstava (kao što su podaci, procesi...).
16. Koriste se mehanizmi koji razgraničavaju kompjuterske sisteme od osnove kompjuterske mreže.
17. Gde god je to moguće, bezbednost se zasniva na tzv. otvorenim standardima radi obezbeđivanja prenosivosti i međudelovanja.
18. Koristi se opšti jezik u razvoju zahteva za bezbednost.
19. Osmišljavaju se i primenjuju mehanizmi provere za otkrivanje neovlašćenog korišćenja i radi sprovođenja istražnih radnji kod bezbednosnih izgreda.
20. Osmišljava se bezbednost da se omogući propisno obnavljanje i prilagođavanje na nove tehnologije što podrazumeva logičan, bezbedan i jednostavan postupak nadogradnje.
21. Otkrivaju se i beleže svi korisnici i procesi koji pristupaju sredstvima SCC d.o.o. Beograd.
22. Koriste se jedinstveni pokazatelji kako bi se osigurao jednoznačan uvid u količinu i način korišćenja IT sredstava.
23. Primenjuje se najmanja moguća mera ovlašćenja za pristup IT sredstvima.
24. Ne uvode se nepotrebni bezbednosni mehanizmi.
25. Informacije se štite tokom njihove obrade, premeštanja i u skladištu.
26. Razvijaju se i primenjuju odgovarajući planovi oporavka od bezbednosnih proboja.
27. Preispituju se svi nabavljeni proizvodi i usluge kako bi se osigurala odgovarajuća bezbednost.
28. Osigurava se pristojna bezbednost za isključene, pokvarene ili izbačene sisteme.
29. Štiti se od svih aktivnosti koje liče na napade, bez obzira da li to jesu.
30. Ustanovljavaju se i sprečavaju opšte greške i ranjivosti

U Beogradu,

05.08.2022.

Ismar Sinanović, dipl.inž.el

ISMS menadžer