641.

Na osnovu člana 68 stav 2 Zakona o tajnosti podataka ("Službeni list CG", br. 14/08 i 76/09), Vlada Crne Gore, na sjednici od 1. jula 2010. godine, donijela je

UREDBA

O BLIŽIM USLOVIMA I NAČINU SPROVOĐENJA INFORMATIČKIH MJERA ZAŠTITE TAJNIH PODATAKA

("Službeni list Crne Gore", br. 057/10 od 01.10.2010)

Član 1

Državni organ, organ državne uprave, organ jedinice lokalne samouprave i drugo pravno lice kojem je povjereno vršenje javnih ovlašćenja (u daljem tekstu: organ), kao i pravno i fizičko lice koje u vršenju zakonom utvrđenih poslova, odnosno izvršavanju ugovorenog posla koristi tajne podatke, a koji planiraju da koriste komunikaciono-informacione sisteme i procese za tajne podatke, dužni su da od Direkcije za zaštitu tajnih podataka pribave certifikat za komunikaciono-informacione sisteme i procese.

Član 2

Uz zahtjev za certifikovanje komunikaciono-informacionog sistema i procesa za tajne podatke (u daljem tekstu: sistem) organ, odnosno pravno ili fizičko lice iz člana 1 ove uredbe prilaže procjenu mogućeg ugrožavanja bezbjednosti tajnih podataka od upada u sistem i upotrebe i uništavanja tajnih podataka koji su obrađeni i čuvani u sistemu (u daljem tekstu: procjena rizika bezbjednosti sistema).

Procjena rizika bezbjednosti sistema odnosi se na utvrđivanje rizika, procjenu rizika koji se ne mogu izbjeći, procjenu ranjivosti sistema, prijetnje i moguće posljedice realizacije pojedinih prijetnji, uključujući i rizike u vezi sa okruženjem u kojem se sistem koristi.

Procjena rizika bezbjednosti sistema vrši se periodično, u skladu sa postupcima za procjenu rizika predviđenim planom za procjenu rizika sistema.

Član 3

Ako organi, pravna ili fizička lica iz člana 1 ove uredbe, imaju potrebu da povežu svoje sisteme, dužni su da zaključe sporazum o povezivanju tih sistema.

Sporazum iz stava 1 ovog člana prilaže se uz zahtjev iz člana 2 stav 1 ove uredbe.

Član 4

Ako Direkcija za zaštitu tajnih podataka (u daljem tekstu: Direkcija) utvrdi da je procjena rizika bezbjednosti sistema sačinjena u skladu sa mjerama zaštite tajnih podataka u sistemu, organ, odnosno pravno ili fizičko lice iz člana 1 ove uredbe prilaže i:

- izjavu o bezbjednosnim potrebama sistema i
- bezbjednosne procedure za prijem, obradu, prenos, čuvanje i arhiviranje tajnih podataka u elektronskoj formi (u daljem tekstu: operativne procedure za bezbjednost sistema).

Način pripreme i sadržaj dokumentacije iz člana 2 stav 1 ove uredbe i stava 1 ovog člana bliže propisuje organ državne uprave nadležan za poslove odbrane.

Član 5

Operativne procedure za bezbjednost sistema odnose se na prostor, prostorije, odnosno bezbjednosne zone u kojima se obrađuju tajni podaci u sistemu, ovlašćena lica za upravljanje bezbjednošću sistema, uslove koje mora da ispunjava sistem, režim rada sistema, kripto zaštitu sistema, zaštitu podataka prilikom obrade i čuvanja u sistemima, zaštitu od rizika kompromitujućeg elektromagnetnog zračenja (u daljem tekstu: KEMZ) i instaliranje uređaja za čuvanje tajnih podataka.

Član 6

Prostor, prostorije, odnosno bezbjednosne zone u kojima se obrađuju tajni podaci u sistemu određuju se u skladu sa propisom o bližim uslovima i načinu sprovođenja mjera zaštite tajnih podataka.

Član 7

Ovlašćena lica za upravljanje bezbjednošću sistema u organu i pravnom licu ili kod fizičkog lica iz člana 1 ove uredbe kontrolišu i ocjenjuju promjene koje utiču na bezbjednost sistema.

Prilikom određivanja ovlašćenih lica za upravljanje bezbjednošću sistema, organi, pravna i fizička lica iz člana 1 ove uredbe, dužni su da obezbijede da jedno lice ne kontroliše sve važne elemente bezbjednosti sistema.

Član 8

Sistem mora ispunjavati uslove za:

- identifikovanje i pouzdano garantovanje identiteta (autentifikacija) lica koja imaju pristup sistemu;
- kontrolu i vođenje evidencije o pristupu sistemu na osnovu ovlašćenog pristupa određenoj bazi podataka;
- kontinuirani zapis o bezbjednosnom stanju sistema (bezbjednosni zapisi), aktivnost sistema, izmjenama postojećeg stanja sistema i sl.;
- proučavanje bezbjednosnih zapisa od strane ovlašćenih lica ;
- određivanje ovlašćenja korisnicima u vezi sa bezbjednošću sistema;
- određivanje ovlašćenja korisnicima u vezi sa pravilnim korišćenjem sistema;
- obezbjeđivanje bezbjednog načina označavanja stepena tajnosti;
- identifikaciju korisnika koji vrši izmjene, štampanje, presnimavanje ili brisanje tajnog dokumenta;
- bezbjednu evidenciju izmjene, štampanja, presnimavanja ili brisanja tajnog podatka od strane korisnika i
- zaštitu važnih tehničkih i programskih elemenata, sistemskih mogućnosti i njegove funkcionalnosti.

Član 9

Sistemi mogu da rade u jednom od sljedećih bezbjednosnih režima:

- "DEDICATED"
- "SYSTEM HIGH"
- "MULTI LEVEL".

Starješina organa, odgovorno lice u pravnom licu i fizičko lice će pisanim aktom odrediti bezbjednosni režim rada sistema.

Član 10

U sistemu koji radi u "DEDICATED" bezbjednosnom režimu rada sva lica koja imaju pristup tom sistemu moraju imati dozvolu za pristup tajnim podacima najvećeg stepena tajnosti podataka koji se obrađuju u sistemu i imaju pristup svim podacima koji se obrađuju u sistemu u skladu sa principom "potrebno je da zna".

U sistemu koji radi u "SYSTEM HIGH" bezbjednosnom režimu rada sva lica koja imaju pristup tom sistemu moraju imati dozvolu za pristup tajnim podacima najvećeg stepena tajnosti podataka koji se obrađuju u sistemu i mogu pristupati samo određenim tajnim podacima u skladu sa principom "potrebno je da zna".

U sistemu koji radi u "MULTI LEVEL" bezbjednosnom režimu rada lica koja imaju pristup tom sistemu ne moraju imati dozvolu za pristup tajnim podacima najvećeg stepena tajnosti podataka koji se obrađuju u sistemu, i imaju pristup samo određenim podacima koji se obrađuju u sistemu, u skladu sa principom "potrebno je da zna".

Selektivan pristup sistemu i selektivan pristup podacima razvijaće se pomoću hardvera i softvera.

Član 11

Tajni podatak ne smije se prenositi kroz sisteme izvan bezbjednosnih zona bez primjene metoda i sredstava kripto zaštite.

Član 12

Izrada, distribucija i čuvanje kripto ključeva i drugog kripto materijala za razmjenu tajnih podataka sa stranim državnim i međunarodnim organizacijama vrši se u skladu sa međunarodnim sporazumima.

Član 13

Radi održavanja potrebnog nivoa bezbjednosti i zaštite sistema u toku njegovog korišćenja, organ, odnosno pravno ili fizičko lice iz člana 1 ove uredbe sprovodi:

- periodičnu provjeru sistema i svih njegovih komponenti, kao i prenosivih medija za čuvanje podataka sa aspekta povjerljivosti, cjelovitosti i dostupnosti;

- zapisivanje podataka koji se odnose na sistem, kao i tajnih podataka koji se obrađuju u sistemu, na zasebnim prenosivim memorijskim medijima i njihovo čuvanje na rezervnim mjestima srazmjerno najvećem stepenu tajnosti podataka;
- instaliranje softvera i konfigurisanje sistema od strane ovlašćenih lica;
- primjenjivanje novih tehničkih i programskih sredstava u sistemu u skladu sa uslovima certifikovanja;
- servisiranje i popravku sredstava iz sistema na način koji ne narušava bezbjednost sistema, u skladu sa uslovima certifikovanja;
- periodičnu zamjenu kripto ključeva i drugog kripto materijala i
- pregled i, po potrebi, zaštitu sredstava iz sistema koja su bila na servisiranju i popravci od KEMZ-a.

Član 14

Prenosiva komunikaciono-informaciona sredstva i memorijski mediji/koji se koriste u sistemu, smatraju se tajnim podatkom i mogu se uključiti u sistem samo ako su certifikovani kao dio sistema.

Član 15

Prenosivi memorijski medij za zapis tajnih podataka koji se koristi u sistemu označava se najvećim stepenom tajnosti, kojim je označen tajni podatak sadržan na njemu.

Član 16

Prenosivi memorijski mediji koji obezbjeđuju pristup sistemu (šifre, lozinke, elementi identifikacije u otvorenoj formi) štite se mjerama koje odgovaraju mjerama zaštite najvećeg stepena tajnosti podataka koji se nalaze u sistemu.

Član 17

Privatna komunikaciono-informaciona sredstva i prenosivi memorijski mediji (lični kompjuteri, prenosivi kompjuteri, diskete, memorijski moduli i sl.) ne mogu se koristiti za obradu tajnih podataka.

Član 18

Ako se tajnom podatku stepena tajnosti "STROGO TAJNO" ili "TAJNO" promijeni ili ukine stepen tajnosti, memorijskom mediju na kojem je taj podatak bio zapisan, ne može se promijeniti ili ukinuti stepen tajnosti.

Ako se tajnom podatku stepena tajnosti "POVJERLJIVO" ili "INTERNO" promijeni ili ukine stepen tajnosti, memorijskom mediju na kojem je taj podatak bio zapisan, može se promijeniti ili ukinuti stepen tajnosti, samo kad je taj podatak izbrisan na način da ga je nemoguće obnoviti softverskim alatom koji odobri Direkcija.

Memorijski mediji iz st. 1 i 2 ovog člana moraju se uništiti nakon isteka roka njihove upotrebe ili nakon isteka roka upotrebe sistema u kojem su se koristili, u skladu sa propisom o bližim uslovima i načinu sprovođenja mjera zaštite tajnih podataka.

Član 19

Tehnički zastarjeli ili oštećeni memorijski mediji na kojima su čuvani tajni podaci uništavaju se u skladu sa propisom o bližim uslovima i načinu sprovođenja mjera zaštite tajnih podataka.

Član 20

Korišćenje automatizovanih komunikaciono-informacionih sredstava koja rade bez prisustva operatera zasniva se na procjeni rizika bezbjednosti sistema.

Član 21

Sve komponente sistema koje se koriste za obradu tajnih podataka stepena tajnosti "POVJERLJIVO", "TAJNO" ili "STROGO TAJNO" moraju biti zaštićene od KEMZ-a, korišćenjem KEMZ protivmjera, u skladu s procjenom rizika od KEMZ-a.

Član 22

Instaliranje uređaja u sistemu vrši ovlašćeno lice u skladu sa operativnim procedurama za bezbjednost sistema.

Član 23

Ako se tajni podaci razmjenjuju sa stranom državom ili međunarodnom organizacijom, može se zahtijevati ispunjenje standarda ili uslova za bezbjednost mreža, uređaja za prenos, međusobne povezanosti sistema i kripto zaštite tajnih podataka u skladu sa međunarodnim sporazumom ili protokolom.

Član 24

Direkcija, u postupku certifikovanja, na osnovu dokumentacije iz čl. 2, 3, 4 i 23 ove uredbe, vrši bezbjednosnu provjeru sistema.

Direkcija izdaje certifikat za sistem, ako su informatičke mjere zaštite potpuno i adekvatno sprovedene.

Certifikat iz stava 2 ovog člana važi tri godine.

Ako Direkcija utvrdi da informatičke mjere zaštite nijesu sprovedene u skladu sa ovom uredbom, odbiće zahtjev za certifikovanje sistema.

Izuzetno, Direkcija može izdati privremeni certifikat za sistem, ako se u postupku certifikovanja sistema utvrdi da sistem ispunjava minimalne bezbjednosne uslove, koji važi do ispunjenja svih uslova, a najduže šest mjeseci od izdavanja.

Član 25

Certifikat se izdaje za sisteme u kojima se obrađuju, prenose i čuvaju tajni podaci stepena tajnosti "POVJERLJIVO", "TAJNO" i "STROGO TAJNO".

Za sisteme u kojima se obrađuju tajni podaci koji su označeni stepenom tajnosti "INTERNO", organi, pravna ili fizička lica iz člana 1 ove uredbe dužni su da obezbijede održavanje adekvatnog nivoa bezbjednosti tajnih podataka (povjerljivosti, cjelovitosti ili dostupnosti), u skladu sa propisima kojima se uređuje informaciona bezbjednost.

Provjeru sprovođenja adekvatnog nivoa bezbjednosti iz stava 2 ovog člana, vrši organ, pravno ili fizičko lice iz člana 1 ove uredbe u saradnji sa Direkcijom.

Član 26

Ova uredba stupa na snagu osmog dana od dana objavljivanja u "Službenom listu Crne Gore".

Broj: 03-6094

Podgorica, 1. jula 2010. godine

Vlada Crne Gore

Predsjednik,

Milo Đukanović, s.r.