PREDLOG

ZAKON
O IZMJENAMA I DOPUNAMA ZAKONA O INFORMACIONOJ BEZBJEDNOSTI

Član 1

U Zakonu o informacionoj bezbjednosti („Službeni list CG“, broj 14/10) u članu 11 st. 1 i 2 riječ „CERT“ zamjenjuje se riječju „CIRT“.

Član 2

U članu 12 stav 2 briše se.

Član 3

U članu 13 stav 1 riječi: “CERT usklađuje postupanje” zamjenjuju se riječima: ”CIRT koordinira radom”.

Poslije stava 1 dodaje se novi stav koji glasi:

“Organi i druga pravna lica iz člana 3 ovog zakona, dužni su da odrede lica zadužena za uspostavljanje sistema zaštite od računarskih i bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti tih sistema, koji će neposredno sarađivati sa CIRT-om radi usklađivanja postupanja tih organa i pravnih lica u primjeni mjera informacione bezbjednosti u slučaju iz stava 1 ovog člana.”

Član 4

Poslije člana 13 dodaje se novi član koji glasi:

“Savjet za informacionu bezbjednost

Član 13a

Radi unaprjeđenja mjera informacione bezbjednosti, kao i praćenja rada i predlaganja aktivnosti CIRT-u na uspostavljanju sistema zaštite od računarskih i bezbjednosnih incidenata na internetu, starješina organa državne uprave nadležnog za informaciono društvo obrazuje savjet za informacionu bezbjednost.

Savjet iz stava 1 ovog člana, čine predstavnici organa državne uprave nadležnog za unutrašnje poslove, organa državne uprave nadležnog za poslove odbrane, organa državne uprave nadležnog za poslove pravosuđa, organa uprave nadležnog za tajne podatke i Agencije za nacionalnu bezbjednost, a po potrebi i predstavnici drugih organa i institucija.

Zadaci savjeta za informacionu bezbjednost utvrdiće se aktom o njegovom obrazovanju.”

Član 5

Poslije člana 14 dodaje se novi član koji glasi:

„Kritična informatička infrastruktura

Član 14a

U cilju zaštite kritične informatičke infrastrukture, organ državne uprave nadležan za informaciono društvo preduzima mjere zaštite te infrastrukture.

Kritičnu informatičku infrastrukturu čine informacioni sistemi organa čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa.

Kritičnu informatičku infrastrukturu i način njene zaštite propisuje Vlada Crne Gore.“

Član 6

Poslije člana 17 dodaje se novi član koji glasi:

„Član 17a

Propis iz člana 14a stav 3 ovog zakona, donijeće se u roku od šest mjeseci od dana stupanja na snagu ovog zakona.“

Član 7

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u „Službenom listu Crne Gore“.

<u>Tekst odredaba Zakona koje se mijenjaju</u>
Obaveza primjene

III SISTEM ZAŠTITE OD RAČUNARSKIH BEZBJEDNOSNIH INCIDENATA

Koordinacija prevencije i zaštite

Član 11

Koordinaciju prevencije i zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema organa i drugih pravnih i fizičkih lica iz člana 3 ovog zakona vrši organ državne uprave nadležan za informaciono društvo, preko posebne organizacione jedinice (u daljem tekstu: CERT).

CERT preduzima mjere za:

1) uspostavljanje sistema zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema organa i drugih pravnih i fizičkih lica iz člana 3 ovog zakona;
2) prevenciju računarsko-bezbjednosnih incidenata;
3) otklanjanje posljedica u slučaju bezbjednosnih incidenata na internetu koji prelaze okvire djelovanja informacionih sistema organa i drugih pravnih i fizičkih lica iz člana 3 ovog zakona.

Organizovanje zaštite pojedinačnih informacionih sistema

Član 12

Organi i druga pravna i fizička lica iz člana 3 ovog zakona mogu organizovati prevenciju i zaštitu svojih informacionih sistema od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti tih sistema.

CERT usklađuje rad organa i drugih pravnih i fizičkih lica iz stava 1 ovog člana.

Usklađivanje postupanja u slučaju računarskih incidenata

Član 13

U slučaju nastanka bezbjednosnih računarskih incidenata na informacionim sistemima organa i drugih pravnih i fizičkih lica iz člana 3 ovog zakona, CERT usklađuje postupanje tih organa u primjeni mjera informacione bezbjednosti.