Komentari Hrvatskog Telekoma d.d.

u okviru javne rasprave o prijedlogu Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga

- Zagreb, 23. srpanj 2012. godine -

UVODNO

U okviru javne rasprave koju je Hrvatska agencija za poštu i elektroničke komunikacije (dalje u tekstu: HAKOM) otvorila dana 13. lipnja 2012. godine o prijedlogu Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (dalje u tekstu: Pravilnik), Hrvatski Telekom d.d. (dalje: HT) ovim putem dostavlja svoje komentare. Ujedno, ovim putem predlažemo da HAKOM po primitku istih organizira sastanak na kojem bi se dodatno usmeno raspravili pojedini članci Pravilnika te time pridonijelo kvaliteti rasprave.

U slučaju potrebe za dodatnim pojašnjenjima, stojimo Vam na raspolaganju.

OSNOVNI KOMENTARI I PRIJEDLOZI NA POJEDINE ODREDBE

1. Članak 2., točke 5. i 10. –Pojmovi i značenja: „kompromitirani informacijski sustav“ i „sigurnosni incident“

Prijedlog: u prijedlogu Pravilnika detaljnije obrazložiti značenja navedenih pojmova.

2. Članak 3., stavci 1. i 5. – Mjere za zaštitu sigurnosti i integriteta mreža i usluga;

Odredbom članka 3., stavak 1. prijedloga Pravilnika propisano je da operatori moraju provesti odgovarajuće tehničke i ustrojstvene mjere za osiguranje sigurnosti i integriteta svojih javnih komunikacijskih mreža i/ili usluga. Međutim, nigdje u tekstu prijedloga Pravilnika nije jasno definirano koje bi to odgovarajuće mjere bile, već se samo opisuju procedure koje je potrebno uključiti u navedene mjere. HT je mišljenja da bi Pravilnikom trebalo jasnije definirati mjere koje treba poduzeti u prijedlogu Pravilnika navedenim slučajevima sve kao bi se izbjegla situacija u praksi da svaki operator elektroničkih komunikacijskih usluga na tržištu provodi drugačije i sadržajno različite mjere. Pozivanje Pravilnika na referentne norme ISO 2700172 i ISO 27005, koji u praksi predstavljaju samo smjernice, može operatorima dati samo okvir ali ne i unificirane mjere koje bi na jednak način i pod jednakim uvjetima bile primjenjive za sve operatere.

Također, odredbom članka 3., stavak 5. prijedloga Pravilnika definirana je obveza operatora da elektroničkim putem jednom godišnje, najkasnije do kraja mjeseca siječnja dostave HAKOM-u dokumentiranu sigurnosnu politiku koja obuhvaća poduzete mjere sigurnosti i pripadajuće norme za prethodnu godinu. I u ovom slučaju nije u potpunosti jasna obveza koju bi operatori bili dužni ispuniti, odnosno, nije jasno što je to točno što bi operatori bili u obvezi dostavljati HAKOM-u elektroničkim putem jednom godišnje, najkasnije do kraja mjeseca siječnja

Prijedlog: Molimo detaljnije obrazloženje obveza iz odredbe članka 3., stavci 1. i 5. prijedloga Pravilnika.

Također, predlaže se izmjena odredbe članka 3., stavak 5, na način da ista glasi:

„Operatori su obvezni elektroničkim putem jednom godišnje, najkasnije do kraja mjeseca siječnja dostaviti Agenciji dokumentiranu sigurnosnu politiku za prethodnu godinu koja obuhvaća mjere

sigurnosti i pripadajuće norme . Izvještaj će se dostavljati upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku. „

3. Članak 4., stavci 1., 2. i 4. – Obavještavanje HAKOM-a o sigurnosnim incidentima;

Odredbom članka 4., stavak 1., točka 4.a. prijedloga Pravilnika propisana je obveza operatora da obavijeste HAKOM o svakom sigurnosnom incidentu koji utječe na ostvarivanje, odnosno primanje ili točno usmjeravanje žurnih poziva. Iz navedene odredbe nije jasno u kojim slučajevima bi operatori bili obvezni ispunjavati navedenu obvezu, naročito zbog toga što prijedlogom Pravilnika nije točno definiran pojam i značenje „žurnih poziva".

Odredbom članka 4., stavak 2., prijedloga Pravilnika propisana je obveza operatora da o sigurnosnim incidentima moraju obavijestiti HAKOM bez odgode, čim su podaci dostupni, i to putem obrasca propisanog u Dodatku 3. Prijedloga Pravilnika:

1. u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, odnosno isteka minimalnog trajanja sigurnosnog incidenta iz Dodatka 2,

2. u roku od najviše 1 sat nakon otklanjanja sigurnosnog incidenta,

3. u roku od najviše 20 dana od dana otklanjanja sigurnosnog incidenta.

Nejasno su i kontradiktorno definirani rokovi u kojima operatori imaju obvezu da o sigurnosnim incidentima obavijeste HAKOM. Stoga smatramo da je navedene rokove potrebno jasnije precizirati kako bi se navedena obveza u praksi mogla točno ispunjavati od strane operatora i kako ne bi došlo do različitih tumačenja koje ni bi bile u skladu sa svrhom koju je HAKOM predmetnom odredbom prijedloga Pravilnika namjeravao postići.

Odredbom članka 4., stavak 4., propisano je da se sve obavijesti o sigurnosnim incidentima moraju se dostaviti HAKOM-u elektroničkim putem na adresu elektroničke pošte incidenti@hakom.hr ili na drugi prikladan način sukladno obrascu iz Dodatka 3 iz prijedloga Pravilnika.

Prijedlog: detaljnije obrazložiti obveze iz odredbi članka 4., stavci 1. i 2. prijedloga Pravilnika te točno definiranje pojma „žurni pozivi".

Također, predlažemo dopuniti odredbu članka 4., stavak 4. prijedloga Pravilnika slijedećom rečenicom: „Obavijesti o sigurnosnim incidentima trebaju biti dostavljene sigurnim komunikacijskim kanalom ili u šifriranom obliku."

4. Članak 5., stavak 1., točke 1. i 2. – Obavještavanje drugih subjekata o sigurnosnim incidentima;

Odredbom članka 5., stavak 1. točka 1. propisana je obveza operatora da odmah obavijeste korisnike javnih komunikacijskih usluga o značajnijem prekidu pružanja javnih komunikacijskih mreža i/ili usluga, sukladno kriterijima za izvješćivanje iz Dodatka 2 prijedloga Pravilnika.

Odredbom članka 5., stavak 1. točka 2. propisana je obveza operatora da obavijesti druge operatore o mjerama koje mogu biti poduzete od strane korisnika javnih komunikacijskih usluga kako bi se uklonila prijetnja sigurnosnog incidenta, koje se odnose na terminalnu opremu korisnika, navodeći moguće troškove vezane uz provođenje takvih mjera.

Prijedlog: detaljnije obrazložiti obveze iz odredbi članka 5., stavak 1., točke 1. i 2. prijedloga Pravilnika na način da se jasno precizira pojam i značenje „značajnijeg prekida pružanja javnih komunikacijskih mreža

i/ili usluga," te da se točno definiraju „mjere koje mogu biti poduzete od strane korisnika javnih komunikacijskih usluga kako bi se uklonila prijetnja sigurnosnog incidenta".

5. Dodatak 1. – Minimalne mjere sigurnosti, Sigurnosni incidenti vezani uz Internet i Kriteriji za izvješćivanje;

U Dodatku 2. prijedloga Pravilnika pobliže su propisane mjere sigurnosti, sigurnosni incidenti vezani uz Internet i kriteriji za izvješćivanje, ali i ovom slučaju isti nisu dovoljno jasno definirano kako bi osigurali jednoznačnu primjenu u praksi od strane svih operatora s ciljem osiguranja cjelovitosti svojih mreža i neprekinutog obavljanje usluga koje se pružaju putem tih mreža.

Prijedlog: detaljno i jasno obrazložiti mjere sigurnosti, sigurnosne incidente vezane uz Internet i kriterije za izvješćivanje obveze iz Dodatka 1. prijedloga Pravilnika.