Iskon Internet d.d.
Garićgradska 18; 10 000 Zagreb, Hrvatska
Tel. +385 1 6000 700; Fax +385 1 6000 777

www.iskon.hr
OIB: 36779353407
Žiroračun kod ZABE: 2360000-1101208338

Zagreb, 23.07.2012.

Komentari Iskon Interneta d.d. u javnoj raspravi na Prijedlog Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga

I. Članak 2. st. 1. t. 9. *prijevara krivotvorenjem internetskih stranica („phishing"): „oblik prijevare na internetu koja se izvodi na kompromitiranom informacijskom sustavu krivotvorenjem internetskih stranica neke banke, novčarske institucije i dr."*

Potrebno je proširenje ove definicije ili izmjenu na način da se ne ograničava isključivo na prijevaru „krivotvorenjem internetskih stranica" obzirom da se *„phishing"* prijevare rade ne samo na taj način već i putem elektroničkih poruka i drugih načina kontaktiranja krajnjih korisnika (primjerice putem društvenih mreža), te da se i drugi dio prijevare izvodi ne samo na kompromitiranom informacijskom sustavu već i na legalnom/nekompromitiranom sustavu na kojem se nalaze stranice koje svojim izgledom obično oponašaju web stranice institucije čiji su korisnici predmet *„phishing"* djelovanja. Ovakvom definicijom smatralo bi se da se radi o *phishingu* samo onda kad su po srijedi kompromitirane internetske stranice, a to u praksi najčešće i nije slučaj.

II. Članak 2.st.1.t.13.*zlonamjerni kod ili aplikacija: programski kod s funkcijom nanošenja štete korisnicima javnih komunikacijskih usluga koji je instaliran i aktivan na terminalnoj opremi bez znanja korisnika.*
Ovakva definicija *zlonamjernog koda* nije dovoljna niti posve točna, obzirom da se *zlonamjerni kod* može aktivirati bilo na računalima krajnjih korisnika bilo na terminalnoj opremi, ali ne nužno bez znanja krajnjeg korisnika. Isto tako, njegova funkcija nije nužno niti uvijek nanošenje štete krajnjim korisnicima, već to može biti i nanošenje štete samom operatoru ili nekoj trećoj strani. *Zlonamjerni kod* je svaki programski kod s ciljem nanošenja štete, neovisno o načinu distribucije ili namjerni.

III. Članak 4. st. 1. t. 4. *o svim sigurnosnim incidentima prijavljenim drugim nadležnim javnopravnim tijelima, a. o svakom sigurnosnom incidentu koji utječe na ostvarivanje, odnosno primanje ili točno usmjeravanje žurnih poziva, b. o svakom sigurnosnom incidentu o kojem operator ima saznanja, a koji je povezan s mogućim gubitkom života.*

Iz ovako navedene formulacije nije jasno da li operator u obvezi prijaviti sve sigurnosne incidente koje prijavljuje drugim nadležnim javnopravnim tijelima poput primjerice

Iskon Internet d.d.
Garićgradska 18; 10 000 Zagreb, Hrvatska
Tel. +385 1 6000 700; Fax +385 1 6000 777

www.iskon.hr
OIB: 36779353407
Žiroračun kod ZABE: 2360000-1101208338

nacionalnog CERT-a, ili samo na slučajeve navedene u t. a) i b) ovog članka, te stoga molimo da se u konačnoj verziji navedeno jasnije napiše.

U stavku 2. Istog članka nije jasno u kojem se roku i koja vrsta incidenta treba prijaviti. U Dodatku 2 su definirani kriteriji ali ne i rokovi. Ukoliko je stavak 2. Trebao definirati rokove u odnosu na vrste incidenata opisane u stavku jedan članka 4. potrebno je to preformulirati pa bi stavak 2. primjerice glasiti:
„O sigurnosnim incidentima iz stavka 1. operatori moraju obavijestiti Agenciju bez odgode, čim su podaci dostupni, i to putem obrasca propisanog u Dodatku 3. ovog Pravilnika:
u slučajevima iz st.1. t.1. ovog članka : *u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, odnosno isteka minimalnog trajanja sigurnosnog incidenta iz Dodatka 2, (…)“*

Na isti način, onda je potrebno i dodati rok u kojem je potrebno izvještavati o incidentima opisanim u članku 4. st.1. t.4. U protivnom, potrebno je pojasniti na što se odnose rokovi prijave definirani u tim stavku 2.

Ovom prilikom želimo istaknuti da bi, obzirom na predviđenu razinu incidenata za koje se određuje obveza izvještavanja, bilo nužno da HAKOM osigura prijavu incidenata elektroničkim putem a da to nije kroz email popunjavanjem obrasca u doc formatu, obzirom da informacije koje se razmjenjuju predstavljaju informacije povjerljive prirode, kao i da je broj ovako opisanih incidenata a time i prijava (primjerice kod *phishinga*) relativno velik. Smatramo također da bi osim jednostavnog navođenja ISO standarda koje operatori trebaju primijeniti bilo potrebno osigurati pomoć, savjetovanje i upute u primjeni sigurnosnih standarda kao i primjereno savjetovanje u slučajevima sigurnosnih incidenata, te u tom smislu pružiti operatorima pomoć u rješavanju sigurnosnih incidenata.

Srdačan pozdrav,

Iskon Internet d.d.