Hrvatska agencija za poštu i elektroničke komunikacije
Jurišićeva 13
10000 Zagreb

Zagreb, 18.7.2012.
Klasa: 600-000/12/96
Ur. broj: I10672-650-125-12-115

Predmet: **Mišljenje na Prijedlog *Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (KLASA: 011-02/12-02/09, URBROJ: 376-12/ŽKB-12-01 (MW) od 13. lipnja 2012.)***

Poštovani,

U prilogu Vam šaljemo mišljenje o Prijedlogu *Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (KLASA: 011-02/12-02/09, URBROJ: 376-12/ŽKB-12-01 (MW) od 13. lipnja 2012.)*

S poštovanjem,

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CARNet J. Marohnića bb 10000 ZAGREB

Zvonimir Stanić, dipl. ing.
Ravnatelj

U prilogu: Mišljenje o Prijedlogu *Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (KLASA: 011-02/12-02/09, URBROJ: 376-12/ŽKB-12-01 (MW) od 13. lipnja 2012.)*

a: Josipa Marohnića 5, HR - 10 000 Zagreb / t: +385 1 6661 616 / f: +385 1 6661 615 / e: ured@carnet.hr

PRILOG: Mišljenje o Prijedlogu Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (KLASA: 011-02/12-02/09, URBROJ: 376-12/ŽKB-12-01 (MW) od 13. lipnja 2012.)

Prema čl. 20 Zakona o informacijskoj sigurnosti (ZoIS), Nacionalni CERT "usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima u nastalih Republici Hrvatskoj" i "usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada".

Stoga opseg sigurnosnih incidenata vezanih uz Internet definiranih Dodatkom 2 prijedloga "Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga" obuhvaća sigurnosne incidente u nadležnosti Nacionalnog CERT-a.

Sukladno tome, predlažemo da se dolje navedeni prijedlozi promjena uvrste u obvezujući dio Pravilnika:

1) u čl. 3 "MJERE ZA ZAŠTITU SIGURNOSTI I INTEGRITETA MREŽA I USLUGA" u stavak (3) dodaje se sljedeći tekst:

> *Operatori su dužni kontinuirano provoditi minimalne proaktivne mjere na Internetu definirane u Dodatku 4 kako bi se smanjila mogućnost pojave incidenta.*

2) u čl. 5 "obavještavanje drugih subjekata o sigurnosnim incidentima" u stavak (1) dodaje se točka 3. koja glasi:

> *3. Operatori su dužni Nacionalnom CERT-u prijavljivati incidente tipova navedenih u Dodatku 5, osim u slučaju da je izvor informacije o nastalom incidentu Nacionalni CERT. U oba slučaja operatori se moraju pridržavati reaktivnih mjera definiranih u Dodatku 5 koje su potrebne za rješenje pojedinog incidenta.*
> *Operatori su dužni slati prijave elektroničkom poštom na adresu ncert@cert.hr i pri tome se može koristiti besplatnu ili komercijalnu verziju PGP kriptosustava. Prijava mora sadržavati IP adrese ugroženih informacijskih sustava, tip incidenta i kratki opis. Na zahtjev Nacionalnog CERT-a operatori su dužni dostaviti tražene informacije o incidentima, a koje ne spadaju u korisničke podatke.*
> *U svrhu učinkovite komunikacije, operatori su dužni Nacionalnom CERT-u dostaviti ime i prezime odgovorne osobe ili naziv nadležne službe, telefonski broj, adresu elektroničke pošte i javni PGP kriptografski ključ, kao i sve promjene tih podataka.*

3) radi bolje preglednosti predlažemo da se sve tablice iz dodataka numeriraju i u tekstu jednoznačno referenciraju.

DODATAK 4: MINIMALNE PROAKTIVNE MJERE KOJE JE POTREBNO PROVODITI PRIJE POJAVE SIGURNOSNIH INCIDENATA NA INTERNETU

Tip sigurnosnog incidenta	Proaktivna mjera
Kontrolno-upravljački centar „botneta"	1. Redovno informiranje krajnjih korisnika na vidnom mjestu o načinima zaraze i ulozi „botneta"
Kompromitirani informacijski sustav	1. Kontinuirano ažurirati operativni sustav i instalirane aplikacije koje su u vlasništvu operatera i za koje korisnik nema administratorske ovlasti 2. Onemogućiti sve mrežne usluge koje nisu neophodne za rad informacijskog sustava 3. Operater mora redovito informirati korisnika, koji je vlasnik virtualnog privatnog sustava, o potrebi provođenja mjera navedenih u točkama 1 i 2 na informacijskim sustavima na kojima korisnik ima administratorske ovlasti 4. Opcionalno implementirati tehničke mjere za zaštitu web sjedišta od mogućih kompromitacija (WAF - Web Application Firewall) i/ili IPS (Intrusion Prevention System) za zaštitu svih usluga
Prijevare	-
Nedozvoljene mrežne aktivnosti	1. Implementacija mjera zaštite od automatiziranog napada pogađanjem lozinki
Napadi uskraćivanjem usluge	1. Implementacija tehničkih mjera za mjerenje i analizu strukture i anomalija prometa u mreži 2. Razrađen plan o načinima filtriranja zloćudnog prometa pri napadima uskraćivanjem usluge
Korisnička računala u sustavu „botneta"	1. Redovno informiranje krajnjih korisnika na vidnom mjestu o načinima zaraze, ulozi „botneta" i načinima zaštite od zaraze zloćudnim kodom

DODATAK 5: MINIMALNE REAKTIVNE MJERE KOJE JE POTREBNO PROVODITI NAKON POJAVE SIGURNOSNIH INCIDENATA NA INTERNETU

Tip sigurnosnog incidenta	Reaktivna mjera
Kontrolno-upravljački centar „botneta"	1. Bez odgode izvijestiti Nacionalni CERT putem elektroničke pošte o incidentu 2. U suradnji sa Nacionalnim CERT-om analizirati i ukloniti kontrolno-upravljački centar
Kompromitirani informacijski sustav	1. Bez odgode izvijestiti Nacionalni CERT putem elektroničke pošte o vremenu nastanka i tipu sigurnosnog incidenta te potom o vremenu njegova završetka 2. Analizirati kompromitirani sustav i zlonamjernu aplikaciju 3. Pronaći ranjivosti koje su korištene pri kompromitaciji 4. Dostaviti Nacionalnom CERT-u primjerak zlonamjernog koda zbog analize istog 5. Ukloniti zlonamjeran kod ili aplikaciju 6. Sanirati pronađene ranjivosti informacijskog sustava ili 1. Bez odgode izvijestiti Nacionalni CERT putem elektroničke pošte o vremenu nastanka i tipu sigurnosnog incidenta te potom o vremenu njegova završetka 2. U suradnji sa Nacionalnim CERT-om analizirati i ukloniti zlonamjeran kod ili aplikaciju u slučaju da je operateru potrebna pomoć
Prijevare	1. Informirati bez odgode Nacionalni CERT putem elektroničke pošte o sigurnosnom incidentu
Nedozvoljene mrežne aktivnosti	1. U slučaju uspješnog napada, odnosno pogođenih korisničkih identifikacijskih podataka, postupak je isti kao kod grupe incidenata „Kompromitirani informacijski sustav"
Napadi uskraćivanjem usluge	1. Analizirati strukturu malicioznog prometa 2. Ovisno o rezultatu analize strukture malicioznog prometa, poduzeti moguće mjere za filtriranje prometa 3. Informirati bez odgode Nacionalni CERT putem elektroničke pošte o vremenu početka i načinu napada te potom o završetku istoga 4. Po potrebi zatražiti od Nacionalnog CERT-a koordinaciju sa CERT-ovima u drugim državama
Korisnička računala u sustavu „botneta"	1. Informirati korisnike o postojanju i tipu zaraze na njihovom računalu