Hrvatska agencija za poštu
i elektroničke komunikacije
Jurišićeva 13
10002 Zagreb

Primjedbe na Pravilnik o načinu i uvjetima sprječavanja i suzbijanja zlouporaba i prijevara u pružanju usluga elektroničke pošte

Poštovani,

Povodom otvaranja javne rasprave o Pravilniku o načinu i uvjetima sprječavanja i suzbijanja zlouporaba i prijevara u pružanju usluga elektroničke pošte, u ime Hrvatske akademske i istraživačke mreže – CARNet, dostavljamo Vam usuglašene primjedbe na ovaj pravilnik koje je izradila radna skupina abuse službi hrvatskih pružatelja internetskih usluga , CARNeta, Nacionalnog CERT-a i CERT-a Zavoda za sigurnost informacijskih sustava, a koje su u prilogu ovom dopisu.

S poštovanjem,

Zvonimir Stanić
Ravnatelj CARNet-a

Općenite primjedbe

- Postoje operatori usluga elektroničke pošte koji nisu ISP-ovi. Jesu li i takvi operatori u ovlasti agencije i što s njima?

- Ako se ne uvede definicija dvije razine filtriranja neželjene e-pošte (npr. sistemska i korisnička, globalna i pojedinačna, itd.), veći dio pravilnika postaje neupotrebljiv i tehnički potpuno neizvediv. Predlažemo uvesti pojmove:

    - Sistemska zaštita, nije je moguće isključiti i ona služi za zaštitu funkcionalnosti samog sustava e-pošte, svaka intervencija na ovoj razini može dovesti do ugrožavanja rada samog poslužitelja e-pošte

    - Korisnička zaštita u praksi se provodi kao davanje spam score ocjene umjesto odbijanja poruke, a na temelju te ocjene korisnik podešava zaštitu na nisku ili visoku razinu (odnosno, primanje ili odbijanje tako označene poruke)

Konkretne primjedbe

čl.2 st.1

Dodati precizne definicije operatora usluge elektroničke pošte i operatora elektroničke komunikacijske mreže

čl.2 st.1 t.2

Bolje definirati neželjenu elektroničku poštu, prijedlog poslužiti se definicijama iz Zakona o elektroničkim komunikacijama, NN 73, 26.06.2008: *„elektronička pošta*: svaka tekstovna, glasovna, zvučna ili slikovna poruka odaslana javnom komunikacijskom mrežom, koja se može pohraniti u mreži ili u terminalnoj opremi primatelja poruke sve dok je primatelj ne preuzme“

čl.2 st.1 t.4

Riječ *ugroza* promijeniti u *ugroza usluge elektroničke pošte*

čl.2 st.1 t.6

Promijeniti definiciju tako da se izbaci *bez znanja korisnika* i doda na kraj mogućnost izazivanja štete i samom korisniku.

čl.4

čl.4 trebao bi propisivati mjere zaštite same usluge, a ne korisnika, potonje je propisano u čl.6

čl.4 st.2

Uočene ugroze preformulirati u *uočene ugroze sustava elektroničke pošte.*

čl.4 st.3

Prijedlog izbaciti ovaj stavak.

Ako stavak ostaje, postavljaju se pitanja:

Postoji li potreba da Agencija prikuplja ove podatke? U RH postoje institucije koje se bave računalnim incidentima poput Nacionalnog CERT-a i drugih CERT organizacija. Radi li se o prikupljanju podataka samo o domaćim operatorima iz kojih dolazi spam ili uključuje i informacije o inozemnim operatorima?

Nije sasvim jasno označava li riječ *dostavlja* obavezu ili opciju?

čl.4 st.4

U širem smislu, nije moguće provoditi (odnosno, opravdati potrebne troškove ako jest moguće) filtriranje cjelokupnog smtp prometa na razini operatora mreže; pojasniti da se misli isključivo na filtriranje odlaznog i dolaznog prometa na poslužiteljima e-pošte.

Sintagma *vodeći računa o potrebnom stupnju zaštite i troškovima implementacije* nije sasvim jasna, prijedlažemo propisati konkretno ili izbaciti.

čl.4 st.6

Dodati da u radnoj skupini koja treba propisati detaljnije mjere moraju biti predstavnici operatora usluga elektroničke pošte, operatora elektroničke komunikacijske mreže, Nacionalnog CERT-a ili drugih CERT organizacija.

čl.5 st.1

Izmijeniti tako da smisao bude *operator je u slučaju nedostupnosti propisanih mjera zaštite dužan obavijestiti korisnika na primjeren način, tamo gdje je to tehnički moguće* (npr. prepaid korisnike nije moguće obavijestiti).

čl.6 st.1

Preformulirati tako da se ne može shvatiti kao besplatni antivirus ili antispam softver za korisnike.

Tko procjenjuje trenutno stanje rizika?

Što je sa zaštitom od npr. sms spama?

čl.6 st.2

Ako se koriste RBL-ovi (Real Time Blackhole List), nije moguće pravodobno obavještavati Agenciju o operatorima koji su blokirani, može biti na stotine izmjena dnevno; prijedlog, izbaciti obvezu obavještavanja Agencije i umjesto toga staviti obvezu da je ISP dužan objaviti popis RBL-ova koji se koriste.

Uskladiti odredbe ovog članka sa čl.4 st.2 (izgledaju redundantno, s tim da čl.6 st.2 izgleda bolje definiran).

čl.6 st.3

S obzirom da nije moguće prevenirati slanje spama, preformulirati tako da glasi: *operator po uočenom problemu provodi mjere s ciljem smanjenja ili zaustavljanja daljnjeg odašiljanja neželjene elektroničke pošte…*

čl.7 st.2

izbaciti suvišni dio tako da glasi: *… razumnim potrebama pretplatnika glede zaštite njegove e-pošte.*

čl.7 st.4

Promijeniti tako da se odnosi samo na poruke filtrirane filterom korisničke razine.

čl.7 st.5

Izbaciti u cijelosti, inače za svaki primljeni spam operator šalje još jednu (spam) poruku korisniku.

čl.7 st.6

Promijeniti tako da se odnosi samo na poruke filtrirane filterom korisničke razine.

čl.7 st.7

Promijeniti tako da se odnosi samo na poruke filtrirane filterom korisničke razine.

čl.8 st.1

Definirati što je terminalna oprema, elektronička pošta se može poslati s npr. iPhone uređaja.

čl.8 st.3

Kako obavijestiti korisnike koji nisu poznati (prepaid korisnici)?

Kako osigurati isporuku obavijesti korisniku ako je korisniku usluga onemogućena? (npr. obavijest e-mailom o blokiranju pristupa e-mailu).

čl.8 st.4

Izmijeniti tako da glasi: *operator usluga elektroničke pošte će ponovo omogućiti pristup svojim uslugama u skladu s propisanim kriterijima, odnosno istekom propisane sankcije (14 dana, 30 dana…), a ne odmah po korisnikovom zahtjevu*.

Izbaciti dio *uz uključenu zaštitu od zlonamjernih programa i neželjene pošte* u kojem se traži od operatora da korisniku uključi antispam/antivirus zaštitu bez korisnikovog znanja.

čl.8. st.5

Izbaciti, jer se podrazumijeva da se korisnik na ukidanje usluge može žaliti Agenciji koja može zatražiti očitovanje operatora; također, samo obavještavanje je problematično (v. primjedbe na čl.8 st.3); također, predstavlja presedan jer se ovakva obavijest ne traži za ukidanje drugih pretplatničkih usluga (plin, voda, struja…)