

Hrvatska Agencija za poštu i elektroničke komunikacije
Jurišićeva 13
HR-10 000 ZAGREB



VIPnet d.o.o.
pp 470, 10002 Zagreb
Vrtni put 1
HR - 10000 Zagreb
Tel.: +385 1 46 91 091
Fax: +385 1 46 91 099
e-mail: office@vipnet.hr
www.vipnet.hr
MB: 1402633
Žiro: 2484008-1100341353

Zagreb, 06. ožujka 2008.

PREDMET: Pravilnik o načinu i uvjetima sprječavanja i suzbijanja zlouporaba i prijevара u pružanju usluga elektroničke pošte - javna rasprava

Poštovani,

Nastavno na otvaranje javne rasprave o prijedlogu Pravilnika o načinu i uvjetima sprječavanja i suzbijanja zlouporaba i prijevара u pružanju usluga elektroničke pošte (u nastavku: prijedlog Pravilnika), ovim putem dostavljamo naše komentare i obrazloženja prijedloga za izmjenama Pravilnika:

Temeljem članka 12. stavka 1. i članka 107. stavka 12 Zakona o elektroničkim komunikacijama (Narodne novine br. 73/08), Vijeće Hrvatske agencije za poštu i elektroničke komunikacije donosi slijedeći

PRAVILNIK O NAČINU I UVJETIMA SPRJEČAVANJA I SUZBIJANJA ZLOUPORABA I PRIJEVARA U PRUŽANJU USLUGA ELEKTRONIČKE POŠTE

I. OPĆE ODREDBE

Sadržaj i svrha

Članak 1.

Pravilnikom o načinu i uvjetima sprječavanja i suzbijanja zlouporaba i prijevара u pružanju usluga elektroničke pošte propisuju se način i uvjeti sprječavanja i suzbijanja zlouporaba i prijevара u pružanju usluga elektroničke pošte, zaštite pretplatnika od neželjene elektroničke pošte, te ispunjavanje obveza operatora i pretplatnika u zaštiti elektroničkih komunikacijskih mreža i usluga.



Pitanje: Obzirom na definiciju elektroničke pošte u značenju pojmova iz Čl. 2. Zakona o elektroničkim komunikacijama, da li se ovaj Pravilnik odnosi i na usluge SMS-a i MMS-a?

Pojmovi i značenja

Članak 2.

Prijedlog: Potrebno je definirati termin operatora usluge elektroničke pošte i razlikovati ga od operatora elektroničkih komunikacijskih usluga, obzirom da usluga elektroničke pošte nije definirana kao djelatnost elektroničkih komunikacijskih usluga i mreža.

(1) U smislu ovog pravilnika pojedini pojmovi imaju sljedeće značenje:

1. *Agencija*: Hrvatska agencija za poštu i elektroničke komunikacije,
2. *neželjena elektronička poruka*: svaka poruka za koju ne postoji razlog da se pojavi u poštanskom sandučiću elektroničke pošte pretplatnika,

Pitanje: Obzirom na definiciju elektroničke pošte u značenju pojmova iz Čl. 2. Zakona o elektroničkim komunikacijama, da li se ovaj termin odnosi i na usluge SMS-a i MMS-a, ili samo na elektroničku poštu (e-mail)?

Pitanje: Obzirom da za svaku primljenu poruku elektroničke pošte postoji razlog njezina primitka bez obzira na opravdanost ili točnost adrese primatelja, nužno je detaljnije i jasnije definirati pojam neželjene poruke elektroničke pošte.

3. *tehnički sustavi za pribavljanje privole*: svaki sustav koji služi za pozivanje korisnika elektroničkih komunikacijskih usluga u svrhu ishođenja privole za pristup uslugama s dodanom vrijednosti ili ishođenja privole za promidžbu/prodaju proizvoda i usluga,
4. *ugroza elektroničke pošte*: potencijalni uzrok koji može nanijeti štetu svakom podatku ili komunikacijskom sustavu u kojem se spremaju i/ili prenose podaci,
5. *Zakon*: Zakon o elektroničkim komunikacijama (Narodne novine br.73/08),
6. *zlonamjerni programi*: programi koji ~~bez znanja korisnika~~ terminalne opreme mogu u određenom obliku preuzeti upravljanje terminalnom opremom ili obavljati neke druge radnje koje mogu izazvati štetu na sadržajima i programima koji su pohranjeni u terminalnoj opremi **i samom korisniku usluge elektroničke pošte.**

II. OBVEZE OPERATORA USLUGA ELEKTRONIČKE POŠTE

Mjere zaštite pretplatnika od zlouporaba i prijevара u pružanju usluga elektroničke pošte

Članak 3.

(1) Operatori usluga elektroničke pošte obvezni su osigurati tehničke i organizacijske mjere zaštite svojih usluga od zlonamjernih programa i neželjenih elektroničkih poruka primjereno ugrozi usluga koje pružaju.

(2) Kada je to potrebno operatori usluga elektroničke pošte će mjere zaštite usluga provoditi u suradnji s operatorom elektroničke komunikacijske mreže, te po potrebi i s drugim operatorima elektroničke pošte.

Tehničke mjere zaštite usluga elektroničke pošte

Članak 4.

(1) Operator usluga elektroničke pošte provodi stalni nadzor svoje mreže glede ugroze usluga, te pri tome primjenjuje primjerene tehničke mjere zaštite svojih usluga, imajući pri tome u vidu stupanj potrebne zaštite, te troškove implementacije mjera zaštite.

(2) Uočene ugroze **sustava elektroničke pošte**, kao i saznanja o mogućim rizicima te izvorima rizika i ugroza, na prikladan način dostavlja obavijest operatoru izvoru ugroza, te u suradnji s tim operatorom poduzima tehničke mjere blokiranja utvrđenog izvora ugroza.

(3) ~~Operator usluge elektroničke pošte~~ **CERT** dostavlja Agenciji podatke o **nacionalnim** operatorima iz čije elektroničke komunikacijske mreže se u većoj mjeri pojavljuju zlonamjerni programi i neželjene elektroničke poruke.

Obrazloženje: U RH postoje institucije koje se bave računalnim incidentima poput Nacionalnog CERT-a i drugih CERT organizacija, te bi one bile najrelevantnije i nepristrane pri dostavljanju podataka o nacionalnim operatorima kao izvorima zlonamjernih programi i neželjenih poruka elektroničke pošte

(4) Posebna obveza operatora elektroničke komunikacijske mreže i operatora usluga elektroničke pošte je provođenje zaštite **filtriranjem prometa** u dolaznom i odlaznom smjeru, vodeći pri tome računa o potrebnom stupnju zaštite te troškovima implementacije te zaštite.

Obrazloženje: nije moguće provoditi (odnosno, opravdati potrebne troškove ako jest moguće) filtriranje cjelokupnog „smtp“ prometa na razini operatora elektroničke komunikacijske mreže; moguće je isključivo filtriranje odlaznog i dolaznog prometa na poslužiteljima e-pošte

(5) Pri provođenju zaštite svoje i povezane elektroničke komunikacijske mreže operatori će koristiti metode najbolje prakse za zaštitu pristupa internetu i usluzi elektroničke pošte.

(6) Agencija će poticati operatore usluga elektroničke pošte na suradnju u svezi zaštite usluga elektroničke pošte, na način da će stupanjem na snagu ovog pravilnika pristupiti osnivanju radne skupine za izradu pravila o provođenju mjera zaštite od zlonamjernih programa i neželjenih elektroničkih komunikacija operatora pri provođenju zaštite svojih usluga elektroničke pošte, elektroničkih komunikacijskih mreža i pretplatnika

Komentar: u radnoj skupini koja treba propisati detaljnije mjere moraju biti predstavnici operatora elektroničke pošte, elektroničkih komunikacijskih mreža, i predstavnici Nacionalnog CERT-a ili drugih CERT organizacija

Organizacijske mjere zaštite usluga elektroničke pošte

Članak 5.

(1) U slučaju kada operator elektroničke komunikacijske mreže uoči ugrozu odnosno mogućnost proboja postavljene zaštite, te ako je ta ugroza izvan trenutnih mogućih tehničkih mjera zaštite, upoznat će pretplatnika **na primjeren način, tamo gdje je to tehnički moguće** o postojanju mogućnosti proboja zaštite, te mjerama koje pretplatnik treba poduzeti radi zaštite svojih komunikacija.

Obrazloženje: pretplatnika – korisnika u režimu plaćanja unaprijed (prepaid) nije moguće upoznati ili obavijestiti ukoliko isti nije registriran i ukoliko nisu poznati njegovi kontakt podaci

(2) Operator usluge elektroničke pošte obvezan je osigurati pretplatniku upute vezano uz provođenje mjera zaštite pretplatnikovih komunikacija kao i načine korištenja operatorovih zaštitnih mjera.

Mjere zaštite od neželjene elektroničke pošte (anti-spam mjere)

Članak 6.

(1) Operator usluge elektroničke pošte obvezan je osigurati **besplatnu** zaštitu od neželjene elektroničke pošte pretplatnicima svojih usluga, pri tome će operator odabrati učinkovitu zaštitu ovisno o trenutnom stanju rizika.

Obrazloženje: neophodne antivirusne ili anti-spam softverske programe nije uvijek moguće osigurati besplatno obzirom na činjenicu da su kvalitetni i referentni softverski programi licencirani i dostatno pouzdani

(2) Operator usluga elektroničke pošte ovlašten je filtrirati ili u potpunosti blokirati dolazni promet kad utvrdi da operator iz dolazne mreže ne poduzima učinkovite mjere u smislu sprječavanja takvog prometa, a o čemu će, **sukladno tehničkim mogućnostima**, izvijestiti tog operatora, svoje pretplatnike i **objaviti popis RBL-ova koji se koriste. Agenciju.**

Obrazloženje: ako se koriste RBL-ovi, nije moguće pravodobno obavještavati Agenciju o operatorima koji su blokirani, obzirom na činjenicu da može biti na stotine izmjena dnevno

(3) Operator usluga elektroničke pošte, **sukladno tehničkim mogućnostima**, provodi mjere **s ciljem smanjenja ili zaustavljanja daljnjeg** sprečavanja odašiljanja neželjene elektroničke pošte u mreže drugih operatora i pri tome je obvezan razmjenjivati bitne informacije o opasnostima s drugim operatorima.



Obrazloženje: obzirom da nije moguće preventivno spriječiti slanje spama, nužno je definirati da operator po uočenom problemu provodi mjere s ciljem smanjenja ili zaustavljanja daljnjeg odašiljanja neželjene e-pošte

Članak 7.

(1) Operator usluga elektroničke pošte mora ponuditi mogućnost uključivanja, isključivanja i podešavanja zaštite svojim pretplatnicima od neželjene pošte i zlonamjernih programa.

(2) Podešavanje sustava zaštite mora biti jednostavno i prilagodljivo razumnim potrebama pretplatnika glede zaštite ~~svog računala, odnosno~~ poštanskog sandučića elektroničke pošte.

(3) Pretplatnik mora biti u mogućnosti provjeriti je li zaštita uključena.

(4) Sve poruke elektroničke pošte koje sustav zaštite označi kao neželjenu elektroničku poštu temeljem **filtriranja filterom razine definirane od strane korisnika** spremit će operator elektroničke pošte na za to predviđeno mjesto u posebnu mapu.

Obrazloženje: neželjena elektronička pošta se definira razinom filtriranja koju definira sam korisnik

~~(5) Operator elektroničke pošte dostavit će pretplatniku obavijest o elektroničkoj pošti za koju sustav zaštite je utvrdio da sadrži zlonamjerne programe ili neželjenu elektroničku poštu, te podatke o adresi pošiljatelja elektroničke pošte, adrese primatelja i sažetak poruke.~~

Obrazloženje: ovaj stavak je nužno obrisati, iz dva razloga. Prvi je temeljen na činjenici da se prva razina zaštite od zlonamjernih programa ili neželjene elektroničke pošte vrši u samoj mreži operatora elektroničke pošte, a druga razina na razini pretinca elektroničke pošte korisnika. Time u slučaju aktiviranja opravdane zaštite na prvoj razini – razini mreže, korisniku se ni u kom slučaju ne dostavlja obavijest iz razloga tehničkih ograničenja. S druge strane, predložena odredba je neprimjenjiva u praksi jer bi primjenom iste postigli potpuno neželjen efekat slanja neželjene elektroničke pošte korisniku slanjem neželjene obavijesne elektroničke pošte umjesto stvarne neželjene elektroničke pošte

(6) Operator elektroničke pošte mora na zahtjev pretplatnika omogućiti pregled zadržane elektroničke pošte, koja je označena kao neželjena elektronička pošta **definirana razinom filtriranja koju definira sam korisnik**, na siguran način, te omogućiti pretplatniku brisanje iste.

Obrazloženje: neželjena elektronička pošta se definira razinom filtriranja koju definira sam korisnik

(7) Zadržanu neželjenu elektroničku poštu **definiranu razinom filtriranja koju definira sam korisnik**, operator usluga elektroničke pošte može izbrisati u roku koji ne može biti kraći od 15 dana od dana spremanja u mapu.

Obrazloženje: neželjena elektronička pošta se definira razinom filtriranja koju definira sam korisnik

III. OBVEZE PRETPLATNIKA USLUGA ELEKTRONIČKE POŠTE

Članak 8.

(1) Pretplatnik usluga elektroničke pošte mora, **sukladno tehničkim mogućnostima**, svoju terminalnu opremu zaštititi odgovarajućim programima koji štite od zlonamjernih programa, te redovito obnavljati podatke tih programa kako bi isti bili u mogućnosti održati visoki stupanj zaštite terminalne opreme.

Obrazloženje: na današnjem tržištu prisutna je široka paleta terminalne opreme za slanje i primanje elektroničke pošte (npr. iPhone) te osiguravanje primjerene zaštite odgovarajućim programima nije zajamčeno i ovisi o samoj tehnologiji i dostupnošću odgovarajućih programa za pojedinu terminalnu opremu.

(2) Kad operator usluga elektroničke pošte utvrdi ili dobije dokaz da je pretplatnik usluga elektroničke pošte izvor ugroze ili slanja neželjenih elektroničkih poruka, operator usluga elektroničke pošte može uskratiti, ovisno o razini opasnosti, djelomični ili potpuni pristup uslugama.

(3) Operator usluga elektroničke pošte će izvijestiti pretplatnika, **ukoliko je moguće**, o razlozima djelomičnog ili potpunog onemogućavanja pristupa uslugama, te dati naputak o mjerama koje pretplatnik mora poduzeti radi otklanjanja ugroza na svojoj terminalnoj opremi.

Obrazloženje: pretplatnika – korisnika u režimu plaćanja unaprijed (prepaid) nije moguće upoznati ili obavijestiti ukoliko isti nije registriran i ukoliko nisu poznati njegovi kontakt podaci. Također, slanje obavijesti korisniku kojem je usluga onemogućena nije moguće.

(4) Nakon što pretplatnik ukloni zlonamjerne programe sa svoje terminalne opreme, operator usluga elektroničke pošte će, **u skladu s propisanim uvjetima, odnosno istekom propisane zaštitne blokade usluga u trajanju od najmanje 15 dana** ponovo omogućiti pristup svojim uslugama, **uz ponovni zahtjev korisnika za uključjenju** zaštite od zlonamjernih programa i neželjene pošte.

Obrazloženje: radi osiguranja potpune sigurnosti sustava elektroničke pošte nužno je osigurati dovoljan rok propisane zaštitne blokade usluga u slučaju inkubacije zlonamjernih programa na terminalnoj opremi ili nepotpunog uklanjanja zlonamjernih programa, i po izvršenju ovih radnji korisnik je obavezan ponovno zatražiti postavljanje antispam/antivirus zaštite prilagođene eventualnim novim postavkama terminalne opreme i uz njegovu prethodnu suglasnost.

(5) U slučaju da pretplatnik usluga elektroničke pošte opetovano ugrožava mrežu ili šalje neželjene elektroničke poruke, operator usluga elektroničke pošte može sukladno Zakonu isključiti pretplatnika, te o tome pismeno izvijestiti Agenciju.

IV. PRIJELAZNE I ZAVRŠNE ODREDBE

Stupanje na snagu pravilnika

Članak 9.



(1) Ovaj pravilnik stupa na snagu u roku osam (8) dana od dana objave u »Narodnim novinama«.

Klasa: 011-01/08-01/00019

Urbroj: 376-12-08-1

Zagreb, _____

PREDSJEDNIK VIJEĆA AGENCIJE

Gašper Gaćina, dipl.ing.el.