



AKOS

AGENCIJA ZA KOMUNIKACIJSKA
OMREŽJA IN STORITVE
REPUBLIKE SLOVENIJE

Anton Luka Šijanec
anton@sijanec.eu

Številka: 3821-5/2022/13

Datum: 8. 6. 2023

Zadeva: **Odgovor uporabniku**

Spoštovani,

Agencija za komunikacijska omrežja in storitve Republike Slovenije (v nadaljevanju agencija) je prejela vaš dopis, v katerem ste opozorili na (po vašem mnenju) nedopustno prakso družbe T-2 d.o.o., Verovškova 64a, 1000 Ljubljana, in sicer glede blokiranja vrat/portov. V zvezi s tem ste v bistvenem navedli, da omenjena družba v nasprotju s takrat veljavnim 203. členom ZEKom-1 blokira IP pakete k in od uporabnika, če le-ti vsebujejo metapodatke o TCP ali UDP seji, ki poteka na izbranih številkah vrat (te so tudi navedene na povezavi <https://www.t-2.net/blokada-vrat>). Ponudnik naj strankam tudi ne bi omogočal ukinitve blokad, razen, če stranke za to dodatno plačajo, pa še v tem primeru ne popolnoma. Vašemu zaprosilu za odstranitev omenjenih blokad niso ugodili.

Zaščito dostopa do odprtega interneta zagotavlja že Uredba (EU) 2015/2120 Evropskega parlamenta in Sveta z dne 25. novembra 2015 (v nadaljevanju Uredba), ki v 3. členu končnim uporabnikom prek storitve dostopa do interneta daje pravico do dostopa do informacij in vsebin ter njihovega razširjanja, do uporabe in zagotavljanja aplikacij in storitev ter do uporabe terminalske opreme po lastni izbiri, ne glede na svojo lokacijo ali lokacijo ponudnika storitve oziroma lokacijo, izvor ali cilj informacije, vsebine, aplikacije ali storitve.

Ponudniki storitev dostopa do interneta pri zagotavljanju storitev dostopa do interneta obravnavajo ves promet enako, brez diskriminacije, omejevanja ali motenja ter ne glede na pošiljatelja in prejemnika, vsebino, do katere se dostopa ali ki se razširja, aplikacije ali storitve, ki se uporabljajo oziroma zagotavljajo, ali terminalsko opremo, ki se uporablja.

Prvi pododstavek ponudnikom storitev dostopa do interneta ne preprečuje uvajanja ukrepov za razumno upravljanje prometa. Da bi se takšni ukrepi šteli za razumne, morajo biti pregledni, nediskriminatorni in sorazmerni ter ne smejo temeljiti na poslovnih razlogih, temveč na objektivno različnih zahtevah glede tehnične kakovosti storitev za posamezno vrsto prometa. Takšni ukrepi ne spremljajo posameznih vsebin in se ne izvajajo dlje, kot je to potrebno.

Ponudniki storitev dostopa do interneta ne izvajajo ukrepov za upravljanje prometa, ki presegajo ukrepe iz drugega pododstavka, zlasti pa ne onemogočajo, upočasnjujejo, spreminjajo, omejujejo, motijo ali poslabšujejo posameznih vsebin, aplikacij ali storitev oziroma posameznih vrst vsebin,



aplikacij ali storitev ali diskriminirajo med njimi, razen kolikor je potrebno in le toliko časa, kot je potrebno za:

(a) skladnost z zakonodajnimi akti Unije ali nacionalno zakonodajo, skladno s pravom Unije, ki velja za ponudnika storitev dostopa do interneta, ali z ukrepi, skladnimi s pravom Unije, s katerimi se izvajajo takšni zakonodajni akti Unije oziroma nacionalna zakonodaja, vključno s sodnimi odločbami ali odločbami javnih organov, ki so jim podeljena ustrezna pooblastila;

(b) ohranitev celovitosti in varnosti omrežja, storitev, ki se zagotavljajo prek tega omrežja, ter terminalske opreme končnih uporabnikov;

(c) preprečitev neizbežne preobremenjenosti omrežja ter blažitev posledic izredne ali začasne preobremenjenosti omrežja, pod pogojem, da se enakovredne vrste prometa obravnavajo enako.

Navedena neposredno uporabljiva evropska ureditev je smiselno povzeta tudi v sedaj veljavnem 268. členu ZEKom-2¹, ki dodaja izjeme pri omejevanju internetnega prometa tudi v primeru: nujnih ukrepov v primeru stanj ogroženosti v skladu s 124. členom tega zakona; nujnih ukrepov za omejevanje neželenih komunikacij v skladu z 226. členom tega zakona (neželene komunikacije) in odločbe sodišča.

Upošteva se navedeno pravno ureditev v izhodišču pravilno tolmačite, da imate kot končni uporabnik storitve dostopa do interneta pravico do dostopa do informacij in vsebin, kot tudi do njihovega razširjanja (brez da bi bili pri tem deležni diskriminacije in omejevanja).

Vendar ta pravica končnega uporabnika ni absolutna. Iz razlogov, povzetih v zgoraj citirani ureditvi, imajo namreč ponudniki storitev dostopa do interneta pravico internetni promet onemogočiti ali kako drugače omejiti. Resda le kolikor je to potrebno in le toliko časa, kot je potrebno.

Predpisanih izjem se je v vašem primeru poslužil tudi vaš operater (družba T-2 d.o.o.). S tem v zvezi agencija uvodoma dodaja, da družba T-2 d.o.o. uporabnike o blokiranih portih javno obvešča na povezavi <https://www.t-2.net/blokada-vrat>, kjer tudi pojasnjuje same razloge za tako ukrepanje. Svoje razloge za posluževanja blokad navedenih portov pa je T-2 d.o.o. pojasnil tudi v svojem odgovoru agenciji, kjer je še podrobneje pojasnil, če v grobem povzamemo, da se takih ukrepov poslužuje iz razloga varnostnih tveganj za celovito delovanje svojega omrežja. Navedeni porti se namreč uvrščajo med najpogostejše vektorje napadov in predstavljajo visoko grožnjo za širjenje zlonamernih datotek ali distribuiran napad. Iz tega razloga so na večini navedenih portov izvedene stalne blokade, kar je tudi v skladu z dobro prakso in smernicami priznanih mednarodnih organizacij.

Družba T-2 d.o.o. je blokiranje portov iz varnostnih razlogov vzpostavila tudi v zvezi s porti 25 in 53, ki sta v vašem dopisu še posebej izpostavljena. Vendar je v povezavi z navedenim družba T-2 d.o.o. posebej izpostavila, da blokado navedenih dveh portov vrši le pri dinamičnih IP naslovih. S tem v zvezi je pojasnila, da gostovanje DNS strežnikov in poštnih strežnikov na dinamičnih IP naslovih tehnično

¹ Prej veljavni 203. člen ZEKom-1.



ni smiselno, saj storitev uporabnikom preneha delovati, v kolikor se uporabniku spremeni IP naslov. Ne glede na to pa so dotični protokoli tudi sicer visoko rizični za ojačitveni porazdelitveni napad z onemogočanjem storitve (Amplification DDos). V kolikor pri portu 53 pride do ojačitvenega napada na uporabnikov DNS strežnik, posledično pride do zasičenja uporabnikove linije ter preobremenjenosti T-2 krovnega DNS strežnika, ki je ključen za delovanje storitev celotnega T-2 omrežja. V kolikor pa preko porta 25 pride do prekomernega pošiljanja neželene pošte s strani uporabnikovega IP naslova, se celotni nabor T-2 IP naslovnega prostora svetovno umesti na črno listo in je s tem onemogočeno pošiljanje spletne pošte iz celotnega T-2 omrežja. Tudi iz razloga, ker do poskusov zlorab prihaja na dnevni ravni, je blokiranje navedenih dveh portov (iz varnostnih razlogov oziroma kot ukrep za omejevanje neželenih komunikacij) upravičeno.

Potrebno je izpostaviti, da T-2 d.o.o. stalno blokira porta 25 in 53 le v primeru dinamičnih IP naslovov. S tem v zvezi je T-2 d.o.o. navedel, da bi bilo tehnično spreminjanje blokade na podlagi trenutno dodeljenega dinamičnega IP naslova prezahtevna tehnična implementacija na jedrnih usmerjevalnikih T-2, ki bi predstavljala stalen poseg v samo konfiguracijo jedrnih usmerjevalnikov. Tako bi bila možna le od-blokada vseh naborov dinamičnih IP-jev, s čimer pa bi bila kritično ogrožena celovitost delovanja T-2 omrežja. Iz tega razloga je tudi po mnenju agencije – glede na tehnično naravo dinamičnega IP naslova – tak ukrep upravičen.

Pri tem pa agencija dodaja, da vaša pravica do dostopa do interneta (in uporabe portov 25 in 53) ni kršena, saj vam operater pravico do razširjanja informacij zagotavlja ob uporabi statičnega IP naslova. V takšnem primeru namreč (stalnih) blokad navedenih portov ni, pač pa se te ročno aktivirajo le v primeru zaznanih zlorab². Tako operater zagotavlja, da je ukrep sorazmeren in časovno omejen. Sama (dodatna) plačljivost takšne storitve pa po mnenju agencije ne predstavlja kršitve vaše pravice dostopa do interneta.

Glede na vse navedeno agencija nepravilnosti v zvezi z izvajanjem Uredbe in 268. člena ZEKom-2 ni zaznala, zaradi česar postopka nadzora v vašem primeru ni uvedla.

Lep pozdrav,

Nejc Čuk
Pooblaščenca oseba agencije

² Blokiranje v tej zadevi izpostavljenih portov je tudi sicer vzpostavljena praksa drugih evropskih operaterjev (in drugih evropskih regulatorjev), kot to npr. izhaja iz dokumenta na povezavi: https://www.berec.europa.eu/sites/default/files/files/document_register_store/2017/12/BoR_%2817%29_2_40_Implementation_report_NN_Post_Plenary_clean_def.pdf



Vročiti: - Naslovniku – po el. pošti (anton@sijanec.eu)