



KLASA: UP/I-344-07/23-01/33

URBROJ: 376-05-2-23-07

Zagreb, 6. srpnja 2023.

Na temelju članka 16. stavka 1. točke 25. i članaka 161. i 162. Zakona o elektroničkim komunikacijama (NN br. 76/22), te članka 96. Zakona o općem upravnom postupku (NN br. 47/09 i 110/21), u inspekcijskom postupku pokrenutom po službenoj dužnosti protiv operatora Telemach Hrvatska d.o.o., Josipa Marohnića 1, 10000 Zagreb, OIB: 70133616033, radi kršenja odredbe članka 43. Zakona o elektroničkim komunikacijama (NN br. 76/22), inspektor elektroničkih komunikacija Hrvatske regulatorne agencije za mrežne djelatnosti donosi

RJEŠENJE

- I. Utvrđuje se da trgovačko društvo Telemach Hrvatska d.o.o., Josipa Marohnića 1, Zagreb, postupuje protivno odredbi članka 43. stavku 1. i stavku 2. Zakona o elektroničkim komunikacijama (NN br. 76/22) na način da nadzire SMS promet između krajnjih korisnika i blokira određene vrste SMS poruka koje ne predstavljaju sigurnosni rizik ili napad na elektroničke komunikacijske mreže i usluge te koje mjere nisu nužne za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga.
- II. Zabranjuje se društvu iz točke I. ovog rješenja primjena mjera nadzora SMS prometa i blokade SMS poruka koje ne predstavljaju sigurnosni rizik ili napad na elektroničke komunikacijske mreže i usluge i koje nisu nužne za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga te se nalaže društvu iz točke I. da odmah po primitku rješenja uskladi svoje postupanje s člankom 43. stavkom 2. Zakona o elektroničkim komunikacijama i ukine primjenu takvih mjera nadzora i blokade SMS prometa.
- III. U slučaju nepostupanja po ovom rješenju, odgovornoj osobi izvršenika, izreći će se novčana kazna u iznosu od 7.000,00 eura (slovima: sedam tisuća eura)/52.741,50 kn (slovima: pedeset dvije tisuće sedamsto četrdeset jedna kuna i pedeset lipa)¹. U slučaju daljnjeg neispunjavanja obveze, izreći će se druga, veća novčana kazna.

Obrazloženje

Hrvatska regulatorna agencija za mrežne djelatnosti (dalje: HAKOM) pokrenula je 3. ožujka 2023. godine postupak inspekcijskog nadzora nad trgovačkim društvom Telemach Hrvatska d.o.o., Josipa Marohnića 1, Zagreb (dalje: Telemach) temeljem članka 16. stavka 1. točke 25. i članaka 161. i 162.

¹ Fiksni tečaj konverzije 7,53450

Zakona o elektroničkim komunikacijama (NN br. 76/22, dalje: ZEK), u svezi utvrđivanja postupanja Telemach-a sukladno odredbi članka 43. ZEK-a.

Naime, inspektor je samostalnom provjerom u razdoblju od 24. veljače 2023. do 2. ožujka 2023. slanjem SMS poruka s broja 385 98 xxxx na brojeve 385 95 xxxx i 385 95 xxxx koji se nalaze u Telemach mreži, čiji je sadržaj identičan ili sličan sadržaju poruka koje aplikacije redovito šalju korisnicima prilikom verifikacije korisničkih računa (npr. Facebook, Google, Instagram i sl.) utvrdio kako predmetne poruke nisu isporučene primateljima, dok su istovremeno istim primateljima isporučene poruke sadržaja „Test“ i/ili „Proba“. Primjeri sadržaja poruka koje nisu isporučene su sljedeći: „Account: xxxxxx is your Samsung account verification code“, „Use xxxxx for two-factor authentication on Facebook“ te „xxxxx is your Google verification code“. Poruke istih sadržaja upućene u mreže drugih operatora zaprimljene su bez ograničenja.

U odnosu na spomenute SMS poruke, inspektor je zatražio detaljno očitovanje Telemacha na okolnosti primjene mjera nadzora SMS prometa, svrhe i temelja takvog nadzora te načina postupanja s predmetnim SMS porukama.

Dana 13. ožujka 2023. Telemach je dostavio svoje očitovanje u kojem, u bitnome, ističe kako primjenjuje mjere zaštite svojih korisnika i svoje mreže, a koje se odnose na sprječavanje različitih vrsta poznatih zlouporaba, uključujući putem SMS poruka. U tu svrhu Telemach koristi SMS vatrozid (*eng. firewall*) čija je svrha automatizirani nadzor SMS prometa, uključujući usmjeravanje (*eng. routing*) prometa. Telemach je istaknuo kako su postavke automatskog nadzora implementirane unutar SMS vatrozida te funkcioniraju bez ikakvog ugrožavanja i/ili zadiranja u zajamčenu tajnost komunikacija. Nadalje, [...].

Telemach je u očitovanju napomenuo kako se ne radi o mjerama nadzora i provjere sadržaja, već o automatiziranim postavkama usporedbe [...]. Sustav se primjenjuje u svrhu detekcije potencijalne zlouporabe, odnosno zaštite sigurnosti i cjelovitosti komunikacijske mreže i njezinih korisnika, sprječavanja nedopuštenog usmjeravanja prometa i neželjene elektroničke komunikacije (*eng. spam*). Također, [...]. Telemach je istaknuo da nitko nema pristup sadržaju SMS poruka uključujući administratora vatrozida te da se blokirani SMS-ovi dalje ne pohranjuju, ne obrađuju i da nije moguće otključavanje kodiranih meta podataka.

U odnosu na konkretne poruke, Telemach se očitovao da su od partnera koji šalju različite tipove verifikacijskih poruka (banke, Facebook, Google, Tik Tok i sl.) dobili sadržaj koji je implementiran u SMS vatrozid te sustav, kod usporedbe uzorka teksta, isti uspoređuje sa sadržajem dobivenim isključivo od autoriziranog pošiljatelja.

U prilogu navedenog očitovanja Telemach je dostavio svojevrsnu izjavu dobavljača sustava [...] te je ukratko opisano kako se radi o kodiranom sadržaju SMS poruka koji se ne otkriva korisnicima sustava (ni bilo kojoj trećoj osobi).

Nakon zaprimljenog očitovanja, inspektor je dana 14. ožujka 2023. zatražio dodatno očitovanje u odnosu na razloge uvođenja ovakvog nadzora odnosno pojašnjenje iz kojeg razloga su upravo konkretne poruke predstavljale rizik odnosno opasnost za sigurnost mreža i usluga.

Dana 17. ožujka 2023. Telemach je dostavio svoje dodatno očitovanje u kojem je istaknuo kako su predmetne poruke upućene s MSISDN-a krajnjeg korisnika, a koji pri tome nije autorizirani partnerski kanal, odnosno nije očekivana komunikacija krajnjeg korisnika. Telemach ističe kako je krajnji cilj slanja takvih poruka drugim krajnjim korisnicima dobivanje povjerenja u legitimitet

pošiljatelja pa ju sustav automatizmom identificira i blokira kao *smishing* poruku (skraćenica za “*SMS phishing*”). Drugim riječima, Telemach smatra da blokiranjem navedenih poruka sprječava krađu identiteta krajnjih korisnika te dodatno ističe kako u kontekstu *smishing-a* isti može biti potpomognut zlonamjernim softverom ili internetskim stranicama za prijave. Nadalje, navodi da trenutno blokiranje predmetnih poruka obeshrabruje prevarante u slanju velike količine SMS poruka (*SMS spamming*), čime se postiglo očuvanje sigurnosti cjelokupne elektroničke komunikacijske mreže i usluga.

Telemach u svom očitovanju nastavno na pitanje inspektora vezano za dostavu primjera poruka koje su evidentno utjecale na sigurnost Telemach elektroničke komunikacijske mreže i usluge navodi kako nema primjera poruka jer ne pohranjuje sadržaj poruka i prevenciju obavlja SMS vatrozid. Konačno, Telemach u svom očitovanju navodi da je implementirao SMS vatrozid [...] te ističe pozitivne strane korištenja predmetnog sustava u cilju sprječavanja krađe osjetljivih podataka, a koje krajnji korisnici imaju na svojim telefonima, u aplikacijama i sl. te kao osnovu navedenog postupanja navodi Opću uredbu o zaštiti podataka (GDPR), Direktivu 2022/2555 o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije (NIS 2 Direktiva) i relevantne ENISA dokumente.

S obzirom da je u navedenom očitovanju bilo nejasno što prema navodima Telemacha predstavlja [...] inspektor je zatražio dodatno očitovanje vezano za predmetno te je Telemach 24. ožujka 2023. dostavio pojašnjenje kako se [...].

Na prijedlog Telemacha, a u svrhu dodatnog pojašnjenja načina postupanja i primjene SMS nadzora, dana 27. travnja 2023. održana je usmena rasprava na kojem su predstavnici Telemacha dodatno pojasnili funkcioniranje SMS vatrozida u dijelu koji se odnosi na blokiranje dolaznih SMS poruka [...]. Predstavnik Telemacha je napomenuo kako sustav po njihovu mišljenju zadovoljava sve EU standarde te da je usklađen sa svim pravnim propisima. Isto tako, napomenuto je kako Telemach primjenjuje blokiranje SMS poruka na način [...]. Predstavnica Telemacha je završno ponovila kako se prilikom nadzora ne ulazi u sadržaj SMS poruka te da Telemach mora poduzeti sve kako bi zaštitio svoje krajnje korisnike.

Na usmenoj raspravi predstavica Telemacha predala je u spis Izjavu [...] (dalje: Izjava), [...] organizacije Mobile Ecosystem Forum Ltd, (dalje: MEF) čiji je Telemach član, kao i prezentaciju pod nazivom „*The Mobile Ecosystem Forum (MEF) & System Messaging Anti-Fraud*“. *The Mobile Ecosystem Forum* (Forum mobilnih ekosustava; MEF) predstavlja globalno strukovno udruženje, čiji je cilj promicati međusektorske rasprave i suradnju, a bavi se, između ostalog, i borbom protiv prijevara i zaštitom potrošača.

Prezentacija MEF-a koja je dostavljena u spis uklatko izlaže o organizaciji, ciljevima i načinu rada udruženja. Prezentacija nadalje opisuje tzv. SMS Sender ID Registry programe i njegove rezultate u Ujedinjenom Kraljevstvu, kao i *Business SMS Fraud Framework* koji definira rizike SMS prijave. Prezentacija opisuje na koji način *Business SMS Ecosytem* funkcionira odnosno način osiguravanja autorizirane rute izravno od pošiljatelja prema primatelju poruke te pojašnjava vrste SMS prijave i posljedice odnosno učinke pojedinih vrsta prijave, kojih je ukupno prepoznato 14. Također, prezentacijom je uklatko opisan sadržaj Kodeksa ponašanja čiji su potpisnici članovi MEF-a.

Izjava [...] predstavlja svojevrsni sažetak prezentacije i ističe sve veći problem SMS prijave, posebno zbog korištenja SMS-a u svrhe dvofaktorske autentifikacije. Prema njegovoj Izjavi, u svrhu zaštite korisnika od potencijalnih prijave, potrebno je implementirati SMS vatrozid.

Nakon zaprimanja svih očitovanja te održane usmene rasprave, inspektor je zaključio kako je Telemach postupio protivno odredbi članka 43. stavka 1. i 2. ZEK-a prilikom primjene opisanih mjera nadzora i kontrole SMS poruka. Naime, odredbom članka 43. stavka 1. ZEK-a propisano je da je u svrhu osiguravanja tajnosti elektroničkih komunikacija i pripadajućih prometnih podataka u javnim komunikacijskim mrežama i javno dostupnim komunikacijskim uslugama zabranjeno slušanje, prisluškivanje, pohranjivanje te svaki oblik presretanja ili nadzora elektroničkih komunikacija i pripadajućih prometnih podataka, osim u slučajevima iz članka 52. ZEK-a te u slučajevima utvrđenim posebnim zakonima.

Stavkom 2. istog članka propisana je iznimka od spomenute zabrane kojom je utvrđeno da se zabrana ne primjenjuje na tehničku pohranu podataka koji su nužni za prijenos komunikacije, ni u slučajevima kada je to nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga, ili za otkrivanje tehničkih kvarova i/ili pogrešaka, sigurnosnih rizika ili napada na elektroničke komunikacijske mreže i usluge, ne zadirući pri tome u načela zaštite tajnosti podataka.

Iz dokaza prikupljenih u predmetnom postupku, kao i očitovanja Telemacha, proizlazi kako je Telemach implementirao mjere nadzora sadržaja SMS poruka, bez valjanog opravdanja ili argumentacije iz koje bi proizlazilo da je isto nužno potrebno te dodatno ničim ne opravdava da blokirane SMS poruke predstavljaju sigurnosni rizik ili bilo kakvu vrstu opasnosti za elektroničke komunikacijske mreže ili usluge, a što predstavlja preduvjet sukladno spomenutoj zakonskoj odredbi. Naime, sama činjenica da [...], ne znači istodobno da prijenos ili zaprimanje takvih poruka može potencijalno ugroziti sigurnost mreža ili usluga. Telemach u svojim očitovanjima ni na koji način nije obrazložio konkretni rizik ili opasnost za sigurnost mreža ili usluga, nije obrazložio da bi blokiranje takvih poruka bilo nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga, ili za otkrivanje tehničkih kvarova i/ili pogrešaka, sigurnosnih rizika ili napada na elektroničke komunikacijske mreže i usluge, već navedeno opravdava zaštitom krajnjih korisnika od eventualnih zlouporaba. Telemach se također poziva na obveze koje proizlaze iz GDPR-a, NIS2 Direktive i ENISA-ne dokumente, ne pojašnjavajući zbog kojih to konkretno obveza je ovakav nadzor implementiran.

Nadalje, prezentacija koja je dostavljena u spis, kao i Izjava [...] nije ukazala na opravdanost i zakonitost postupanja Telemacha budući da se isključivo radi o opisu načina na koji se u današnje vrijeme vrše prijave putem SMS poruka. Isto tako, spomenuta Izjava i prezentacija nisu dostavljene od stranke u postupku, već se radi o trećim osobama odnosno udruženju koje nije stranka u postupku.

Iz svega navedenog slijedi da postupanje Telemacha podrazumijeva nadzor SMS prometa koji se, između ostalih parametara, [...]. U postupku je nesporno utvrđeno kako implementirani sustav Telemacha vrši nadzor cjelokupnog SMS prometa odnosno provodi nadzor sadržaja SMS poruka, a primjena automatiziranog nadzora bez ljudskog posredovanja, mjera kriptiranja ili ograničavanja uvida u zapise ne mijenja prethodni zaključak.

Člankom 43. stavkom 2. ZEK-a propisana je iznimka od zabrane nadzora elektroničkih komunikacija i pripadajućih prometnih podataka. Međutim, ta iznimka utvrđena je za konkretne, iznimne slučajeve koji bi morali opravdati primjenu takvih mjera. U konkretnom slučaju ne postoji valjano opravdanje da bi predmetne poruke na bilo koji način utjecale na sigurnost elektroničkih komunikacija i/ili usluga odnosno da bi bio ispunjen bilo koji od uvjeta iz članka 43. stavka 2. ZEK-a koji opravdava iznimku od propisanu stavkom 1. istog članka.

[...]. Stoga je inspektor točkom II. rješenja naložio zabranu primjene mjera nadzora elektroničkih komunikacija predmetnih SMS poruka, kada nisu ispunjeni uvjeti iz članka 43. stavka 2. ZEK-a, a na

način kako je to vršio Telemach. Isto tako, rješenjem je Telemachu naloženo ukidanje primjene postojećih mjera nadzora budući da u postupku nije utvrđena opravdanost primjene opisanih mjera nadzora odnosno blokiranja predmetnih poruka.

Nadalje, inspektor je temeljem članka 142. Zakona o općem upravnom postupku (NN br. 47/09, 110/21) za slučaj nepostupanja po ovom rješenju odgovornoj osobi izvršenika zaprijetio izricanjem novčane kazne u iznosu od 7.000,00 eura (slovima: sedam tisuća eura)/52.741,50 kn (slovima: pedeset dvije tisuće sedamsto četrdeset jedna kuna i pedeset lipa), a za slučaj daljnjeg neispunjavanja obveze, izricanjem druge, veće novčane kazne.

Na temelju svega navedenog odlučeno je kao u izreci.

Ovo rješenje će se na odgovarajući način objaviti na internetskoj stranici HAKOM-a.

UPUTA O PRAVNOM LIJEKU:

Protiv ovog rješenja žalba nije dopuštena. Protiv ovog rješenja može se, u roku od 30 dana od dana njezina primitka, pokrenuti upravni spor pred Visokim upravnim sudom.

INSPEKTOR ELEKTRONIČKIH KOMUNIKACIJA

Andro Marčev dipl. ing. prom.

Dostaviti:

1. Telemach Hrvatska d.o.o., Josipa Marohnića 1, 10000 Zagreb, UP – osobnom dostavom
2. U spis