KLASA: UP/I-344-07/22-01/62
URBROJ: 376-05-22-05
Zagreb, 14. prosinca 2022.

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 41. 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., OIB: 70133616033, nije postupalo sukladno odredbi članka 41. Zakona o elektroničkim komunikacijama (NN br. 76/22).

II. Utvrđuje se da trgovačko društvo Telemach Hrvatska d.o.o., OIB: 70133616033, nije poduzelo odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga u odnosu na pravovremeno dokumentiranje i ažuriranje internih akata, korištenje različitih korisničkih profila kao i različitih poruka identifikacije prilikom pristupa testnoj, predprodukcijskoj i produkcijskoj okolini te nadzor i zaštitu osobnih podataka prilikom korištenja istih u testnoj i predprodukcijskoj okolini.

III. Nalaže se društvu iz točke I. ovog rješenja da se u roku 30 dana od primitka ovog rješenja uskladi s odredbom članka 41. Zakona o elektroničkim komunikacijama (NN br. 76/22) i Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/2021), te da poduzme odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga, odnosno da ukloni utvrđene nedostatke te uskladi svoje poslovanje sukladno Pravilniku o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/2021) i o navedenom dostavi dokaz inspektoru elektroničkih komunikacija Hrvatske regulatorne agencije za mrežne djelatnosti.

IV. U slučaju nepostupanja po ovom rješenju, odgovornoj osobi izvršenika, izreći će se novčana kazna u iznosu od 100.000,00 kn (slovima: sto tisuća kuna). U slučaju daljnjeg neispunjavanja obveze, izreći će se druga, veća novčana kazna.

Obrazloženje

Hrvatska regulatorna agencija za mrežne djelatnosti (dalje: HAKOM) pokrenula je dana 28. listopada 2022. godine postupak inspekcijskog nadzora nad trgovačkim društvom Telemach Hrvatska d.o.o., Josipa Marohnića 1, OIB: 70133616033 (dalje: Telemach) temeljem članka 16. stavka 1. točke 25. i članaka 161. i 162. Zakona o elektroničkim komunikacijama (NN br. 76/22, dalje: ZEK), u svezi utvrđivanja postupanja Telemach-a sukladno odredbi članka 41. ZEK-a i Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21) (dalje: Pravilnik) te je inspektor elektroničkih komunikacija (dalje: inspektor) obavijestio Telemach da će inspekcijski pregled provesti dana 14. studenog 2022. godine u prostorijama Telemach-a.

Tijekom inspekcijskog nadzora inspektor je provjerio usklađenost informacijskog sustava Telemach-a s minimalnim mjerama sigurnosti sukladno Pravilniku, odnosno njegovu usklađenost s mjerodavnim nacionalnim i međunarodnim sigurnosnim standardima, a koji propisuju zahtjeve za sustave upravljanja informacijskom sigurnošću, i to u određenom, manjem opsegu zahtjeva propisanih standardima koji su navedeni kao referentni u Dodatku 1 Pravilnika.

U tom kontekstu inspektor je nadzorom obuhvatio dokumentirane interne akte, odnosno provjeru ima li Telemach dokumentiranu […] (dalje: Politika), kada je zadnji puta ista ažurirana, tko ju je napisao, pregledao i odobrio te koliko često se pregledava te je utvrdio da je Politika dostupna na intranetu pod „Oglasnom pločom“ u kojoj se nalaze sve politike. Politika je usvojena xx.xx. 2021. godine, a stupila na snagu xx.xx. 2022. godine te se ista pregledava jednom godišnje, a što je navedeno u članku 16. Politike. Nadalje, utvrđeno je da ju je izradio Odjel korporativne sigurnosti, pregledao Odjel pravnih i regulativnih poslova, a odobrio Predsjednik uprave, da se ažurira periodično u skladu s promjenama u informacijskom sustavu Telemach-a i njegovoj okolini, u slučajevima narušavanja sigurnosti te ovisno o rezultatima procjene rizika ili revizije informacijskog sustava, a sve sukladno točki 2.3. Politike.

Također, inspektor je provjerio postoji li postupak kojim se osigurava da se prava pristupa korisnika uklone nakon prestanka radnog odnosa, ugovora ili da se prilagođavaju prilikom promjene te je utvrdio da je trenutno je na snazi […] (dalje: *Procedura*), dok je nova u izradi. *Procedura* je izrađena xx.xx. 2018. godine te je posljednji puta ažurirana xx.xx. 2018. godine. Telemach je naveo da se *Procedura* više ne koristi jer je novi sustav xy zamijenio prethodni xy sustav, a što će biti propisano novim […], koji je izrađen xx.xx. 2022. godine, ali nije još odobren. Inspektor je u Odjelu ljudskih resursa nasumično odabrao dva zaposlenika iz sustava koji imaju prekid radnog odnosa unazad 3 mjeseca. Prvi odabrani zaposlenik je xy, za koju je zahtjev za ukidanje prava pristupa podnesen xx.xx. 2022. godine, zbog prekida radnog odnosa koji je nastupio xx.xx. 2022. godine. Inspektor je provjerom utvrdio da je zahtjev za ukidanje domenskih prava pristupa odrađen xx.xx. 2022. godine, dok su xx.xx. 2022. godine brisane licence, prava pristupa sustavima i elektronička pošta zaposlenice. Drugi nasumično odabran zaposlenik je xz, za kojeg je zahtjev za ukidanje prava pristupa kreiran xx.xx. 2022. godine, zbog prekida radnog odnosa koji je nastupio xx.xx. 2022. godine. Inspektor je provjerom utvrdio da je xx.xx. 2022. godine nakon 16 sati ukinut domenski korisnički račun, dok su xx.xx. 2022. godine brisane licence, prava pristupa sustavima i elektronička pošta zaposlenika.

Nadalje, inspektor je provjerio jesu li korisnički računi s privilegiranim pristupom odvojeno upravljani i kontrolirani i zatražio uvid u dokument u kojem je propisana kompleksnost lozinki te je utvrdio da je trenutno na snazi […]koji je posljednji puta ažuriran xx.xx. 2018. godine. Zaposlenici su objasnili da koriste različite vrste korisničkih imena ovisno o sustavima kojima pristupaju te za spajanje na xx, dok za pristup svom računalu koriste korisničko ime i lozinku, a za Windows servere i sve druge servere posebna/različita korisnička imena (admin-username i ad-username i sl.) i lozinke.

Također, inspektor je provjerio postoji li postupak odabira testnih podataka, kopiraju li se i modificiraju podaci s produkcije na testnom okruženju, brišu li se produkcijski podaci odmah nakon testiranja s testnog okruženja, postoje li različiti korisnički profili za produkcijske i testne sustave te razlikuje li se poruka identifikacije prilikom logiranja (menus) za pojedini sustav. Inspektor je prilikom provjere utvrdio da zaposlenica koja radi na sustavu naplate misli da se u testnom okruženju koriste podaci koji su kreirani samo za potrebe testiranja budući da postoji testno, predprodukcijsko i produkcijsko okruženje. Zaposlenica je objasnila da se na predprodukciji rade testiranja prije nego krene produkcija da bi se provjerile nelogičnosti i izbjegli eventualni problemi pogrešnog obračuna te se na predprodukciji koriste podaci s produkcije na način da se „gaze“ više puta tjedno. Inspektor je zaposlenicu zamolio da pretraži prezime xa u produkcijskom okruženju te je nasumično odabrana korisnica xa, […]za koju je utvrđeno da se njeni osobni podaci nalaze i na predprodukcijskom i testnom okruženju. Nadalje, testno, predprodukcijsko i produkcijsko okruženje je razdvojeno i posebno se ulazi u svako okruženje, no ne razlikuje se poruka identifikacije prilikom pristupanja (menus) za pojedini sustav već se okruženje prepoznaje po IP adresi na vrhu sučelja. Zaposlenica je za sva tri okruženja koristila isto korisničko ime te istu složenost lozinke.

Iz svega prethodno navedenog inspektor je zaključio da Telemach nije poduzeo odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga, iz sljedećih razloga. Dokumentiranje i u planiranim intervalima (jednom godišnje) ili prilikom značajnih promjena, ažuriranje pravilnika, odnosno procedura, uputa, politika i drugih internih akata predstavlja preduvjet za osiguranje sigurnosti informacijskog sustava. Telemach nije ažurirao *Proceduru,* odnosno u istoj nisu implementirane promjene sustava koje su na snazi te samim time nije propisano na koji način upravlja pravima pristupa za korisnike te na koji način osigurava da se prava pristupa korisnika uklone nakon prestanka radnog odnosa, ugovora ili da se prilagođavaju prilikom promjene. Također, Telemach od 2018. godine nije ažurirao *Pravilnik* […]te zaposlenici ne koriste različite korisničke profile prilikom pristupa testnom, predprodukcijskom i produkcijskom okruženju sustava naplate budući da se za sva tri okruženja koristi isto korisničko ime te ista složenost lozinke, a što je u suprotnosti sa zahtjevima za očuvanje informacijske sigurnosti nacionalnih i međunarodnih standarda. Također, prilikom pristupanja pojedinom sustavu, odnosno testnom, predprodukcijskom i produkcijskom okruženju poruka identifikacije se ne razlikuje, već se okruženje prepoznaje po IP adresi na vrhu sučelja, a što povećava rizik ljudske greške. Nadalje, osobni podaci korisnika se nemodificirano kopiraju s produkcijske okoline na predprodukcijsku i testnu okolinu te se ti podaci ne brišu s istih nakon provedenog testiranja, a iz čega proizlazi da testni podaci nisu odabrani pažljivo, te da nisu zaštićeni i kontrolirani, odnosno osobni podaci korisnika u ovom slučaju nisu modificirani ili uklonjeni prilikom kopiranja istih s produkcijskog na predprodukcijsko ili testno okruženje. Navedeno je u suprotnosti sa zahtjevima nacionalnih i međunarodnih standarda za očuvanje informacijske sigurnosti, odnosno za sprečavanje zlouporabe osobnih podataka. Svi prethodno utvrđeni nedostaci u suprotnosti su s mjerama sigurnosti koje proizlaze iz mjerodavnim nacionalnih i međunarodnih sigurnosnih standarda (kao npr. ISO 27 001:2013), a koji propisuju zahtjeve za sustave upravljanja informacijskom sigurnošću te su navedeni kao referentne norme za provođenje mjera informacijske sigurnosti u Dodatku 1. Pravilnika.

Nastavno na prethodno navedeni zaključak, inspektor je ovim Rješenjem Telemach-u naložio da se u roku 30 dana od primitka ovog rješenja uskladi s odredbom članka 41. ZEK-a, kao i Pravilnikom te da poduzme odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga, a koje se odnose na pravovremeno dokumentiranje i ažuriranje internih akata, korištenje različitih korisničkih profila kao i različitih poruka identifikacije prilikom pristupa testnoj, predprodukcijskoj i produkcijskoj okolini te nadzor i zaštitu osobnih podataka prilikom korištenja istih u testnoj i predprodukcijskoj okolini, kao i da o navedenom dostavi dokaz inspektoru elektroničkih komunikacija Hrvatske regulatorne agencije za mrežne djelatnosti. Također, nastavno na provedeni inspekcijski nadzor u kojem je nadzor proveden u odnosu na manji dio zahtjeva minimalnih mjera sigurnosti iz Dodatka 1. Pravilnika, inspektor napominje da je Telemach dužan uskladiti svoje cjelokupno poslovanje s Pravilnikom, odnosno ispraviti nedostatke utvrđene Rješenjem, te svoje cjelokupno poslovanje i aktivnosti uskladiti s mjerama informacijske sigurnosti na način propisan ZEK-om i Pravilnikom.

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 100.000 kn (slovima: sto tisuća kuna), 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

Željka Kardum Ban, mag.ing.el., univ.spec.elect.comm., univ. spec.oec.

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