KLASA: UP/I-344-07/23-01/77
URBROJ: 376-05-23-03
Zagreb, 27. rujna 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 nad operatorom Iskon Internet d.d., Radnička cesta 21, 10000 Zagreb, OIB: 36779353407, vezano uz primjenu 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 Iskon Internet d.d., OIB: 36779353407, nije postupalo sukladno odredbi članka 41. Zakona o elektroničkim komunikacijama (NN br. 76/22).

II. Utvrđuje se da trgovačko društvo Iskon Internet d.d., Radnička cesta 21, 10000 Zagreb, OIB: 36779353407, nije poduzelo odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga u odnosu na dokumentiranje internih akata vezanih uz informacijsku sigurnost, ocjenu efikasnosti edukacije o podizanju svijesti o informacijskoj sigurnosti te zadovoljavajuće testiranje funkcionalnosti procesa, procedura i kontrola kontinuiteta informacijske sigurnosti.

III. Nalaže se trgovačkom društvu iz točke I. ovog rješenja da u roku 45 dana od primitka ovog rješenja uskladi svoje poslovanje s odredbom članka 41. Zakona o elektroničkim komunikacijama (NN br. 76/22) i Pravilnikom o načinu i rokovima provedbe mjera zaštite sigurnosti mreža i usluga (NN br. 52/23), na način 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 mreža i usluga (NN br. 52/23), odnosno da ukloni utvrđene nedostatke iz točke II. ovog rješenja 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 10.000 eura (slovima: deset tisuća eura) / 75.345 kuna (slovima: sedamdeset pet tisuća tristo četrdeset pet kuna)[1]. U slučaju daljnjeg neispunjavanja obveze, izreći će se druga, veća novčana kazna.

[1] Fiksni tečaj konverzije 1 EUR = 7,53450 kn

Obrazloženje

Hrvatska regulatorna agencija za mrežne djelatnosti (dalje: HAKOM) pokrenula je dana 15. lipnja 2023. postupak inspekcijskog nadzora nad trgovačkim društvom operatorom Iskon Internet d.d., Radnička cesta 21, 10000 Zagreb, OIB:36779353407 (dalje: Iskon) 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 Iskona sukladno odredbi članka 41. ZEK-a i Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti mreža i usluga (NN br. 52/2023,dalje: Pravilnik) te je inspektor elektroničkih komunikacija (dalje: inspektor) obavijestio Iskon da će inspekcijski pregled provesti dana 7. srpnja 2023. u prostorijama Iskona.

Tijekom inspekcijskog nadzora inspektor je provjerio usklađenost informacijskog sustava Iskona 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 pregledao postupak za vlasnike imovine kojim pregledavaju redovito prava pristupa sustavima te je pregledao *Izvještaj o reviziji prava pristupa 2023 za* […], od […], u kojem su uspoređeni popis zaposlenika iz HR baze i aktivni korisnički računi imeničkog direktorija te je utvrdio da nema odstupanja i nesukladnosti.

Inspektor je provjerio i na koji način SOC (sigurnosni operativni centar) nadzire neuobičajeno ponašanje na sustavima te je na uvid dobio *[…],*u kojem su navedeni: […]. Inspektor je također utvrdio da se nakon […] neuspješnih pokušaja *logiranja* u bazu sustava naplate s […], korisnički podaci automatski blokiraju na […] na imeničkom direktoriju, kao i da SOC bilježi brisanje, promjenu prava pristupa bazi te izvoz podataka iz baze sustava za naplatu.

Inspektor je provjerio i broj zaposlenika koji su zaposleni u 2023., proceduru praćenja edukacija zaposlenika vezanih uz informacijsku sigurnost i postoji li testiranje zaposlenika nakon provedene edukacije te je utvrdio da Iskon na dan […]. , ima […] zaposlenika dok je u 2023. zaposleno […] novih zaposlenika. Svaki zaposlenik prilikom zaposlenja dobije svoj korisnički račun za pristup portalu […] gdje su mu dodijeljene edukacije i rokovi u kojem ih mora proći. Zadnja edukacija o informacijskoj sigurnosti održana je *online* za […] zaposlenika, […] za zaposlenike koji nisu prošli edukaciju o informacijskoj ili fizičkoj sigurnosti. Sama edukacija održana je kao predavanje bez završnog testa. Inspektor je nasumičnim odabirom odabrao dva zaposlenika i to […] zaposlenog […] i […], zaposlenog […]. Za zaposlenika […], utvrđeno je putem sustava da nema zakašnjelih edukacija, te da je prošao edukaciju o informacijskoj sigurnosti […]. kao i *online* edukaciju o informacijskoj sigurnosti […]. Za zaposlenika […] utvrđeno je da nema zakašnjelih edukacija te da je edukaciju o informacijskoj sigurnosti prošao […], dok je online edukaciju o informacijskoj sigurnosti prošao […]. Spomenuti zaposlenici su prvotno bili zaposleni u Iskonu putem agencije te su zato edukaciju o informacijskoj sigurnosti prošli prije zasnivanja radnog odnosa u Iskonu.

Nadalje, inspektor je provjerio postoje li dokumentirani procesi, procedure i kontrole za osiguravanje kontinuiteta informacijske sigurnosti te je utvrdio postojanje *Priručnika za postupanje u kriznim situacijama,* u kojem nije navedeno tko ga je izradio, odobrio i kada je zadnje ažuriran, no navedeno je da je iz 2023., zatim dokumenata *Upravljanje kontinuitetom poslovanja* od […], *Plan testiranja kontinuiteta poslovanja* od […]. u kojem nije navedeno tko je odobrio dokument već samo tko ga je

izradio, *Plan oporavka kritičnih IT servisa* od […]., *Zapisnik o testiranju plana oporavka od katastrofe* od […]. u kojem nije navedeno tko je odobrio dokument, već samo tko ga je izradio te *Zapisnik o testiranju plana kontinuiteta poslovanja* od […]. u kojem nije navedeno tko je odobrio dokument već samo tko ga je izradio. U dokumentu *Zapisnik o testiranju plana kontinuiteta poslovanja* opisano je metodom papirnatog testa testiranje dostupnosti opreme (sustava) za pružanje usluge klijentima uslijed značajnijeg kvara i/ili kibernetičke ugroze, no bez stvarne simulacije neželjenog događaja na način da je tim pregledao korake plana oporavka. Nema zapisa rezultata testiranja redundancije svih kritičnih sustava. U dokumentu *Zapisnik o testiranju plana oporavka od katastrofe* je prikaz provedbe testa oporavka […] sustava uslijed nedostupnosti biling baze gdje je početak kvara bio […]. u […] sati, koji je imao utjecaj na korisnike - poteškoće u radu usluga, u […] je odrađeno prebacivanje na sekundarnu bazu te je u tijeku bilo testiranje provjera, od […] sekundarna baza je aktivirana te su se korisnici mogli spajati, dok je kriza okončana u […]. Testiranje je provedeno na produkcijskom sustavu.

Iz svega prethodno navedenog inspektor je zaključio da Iskon nije u potpunosti poduzeo odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga iz sljedećih razloga. Dokumentiranje i ažuriranje pravilnika, odnosno procedura, uputa, politika i drugih internih akata kao i navođenje autora dokumenta, osoba koja su isti pregledali te odobrili predstavlja preduvjet za osiguranje sigurnosti informacijskog sustava te je jasno propisano međunarodnom važećom normom informacijske sigurnosti ISO 27001. Iskon nije na ispravan način dokumentirao informacije u dokumentima: *Priručnik za postupanje u kriznim situacijama*, u kojem nije navedeno tko ga je izradio, odobrio i kada je zadnje ažuriran, no navedeno je da je iz 2023., *Plan testiranja kontinuiteta poslovanja* od […]. u kojem nije navedeno tko je odobrio dokument već samo tko ga je izradio, *Zapisnik o testiranju plana oporavka od katastrofe* od […] u kojem nije navedeno tko je odobrio dokument, već samo tko ga je izradio te *Zapisnik o testiranju plana kontinuiteta poslovanja* od […]. u kojem nije navedeno tko je odobrio dokument već samo tko ga je izradio. Nadalje, prilikom online edukacije o informacijskoj sigurnosti Iskon nije ocijenio efikasnost edukacije budući da nije bilo završnog testa ili nekog drugog načina ocjene efikasnosti, kao što je to opisano u međunarodnoj važećoj normi ISO 27 002, te se time povećava rizik od nastanka incidenata koji mogu utjecati na sigurnost i cjelovitost mreža i usluga Iskona. Vezano uz testiranje plana kontinuiteta poslovanja, inspektor je utvrdio da Iskon ne testira *[...]*, vidljivo iz dokumenta *Zapisnik o testiranju plana kontinuiteta poslovanja*, a što inspektor smatra da nije zadovoljavajuće testiranje funkcionalnosti procesa kontinuiteta informacijske sigurnosti budući da je testiranje redundancije kritičnih sustava […], sukladno minimalnim mjerama sigurnosti iz Pravilnika.

Nastavno na prethodno navedeni zaključak, inspektor je ovim Rješenjem Iskonu naložio da u roku 45 dana od primitka ovog rješenja uskladi svoje poslovanje 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 dokumentiranje internih akata vezanih uz informacijsku sigurnost, ocjenu efikasnosti edukacije o podizanju svijesti o informacijskoj sigurnosti te zadovoljavajuće testiranje funkcionalnosti procesa, procedura i kontrola kontinuiteta informacijske sigurnosti, kao i da o navedenom dostavi dokaz inspektoru HAKOM-a. Također, nastavno na provedeni inspekcijski nadzor koji je proveden u odnosu na manji opseg zahtjeva propisanih standardima koji su navedeni kao referentni u Dodatku 1 Pravilnika, inspektor napominje da je Iskon 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) za slučaj nepostupanja po ovom rješenju odgovornoj osobi izvršenika zaprijetio izricanjem novčane kazne u iznosu od 10.000 eura (slovima: deset tisuća eura) / 75.345 kuna (slovima: sedamdeset pet tisuća tristo četrdeset pet kuna)[2], 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. Iskon Internet d.d., Radnička cesta 21, 10000 Zagreb, UP-osobnom dostavom
2. U spis

[2] Fiksni tečaj konverzije 1 EUR = 7,53450 kn