KLASA: UP/I-344-07/23-01/76
URBROJ: 376-05-23-05
Zagreb, 22. 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 nad operatorom A1 Hrvatska d.o.o., Vrtni put 1, 10000 Zagreb, OIB:29524210204, 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 A1 Hrvatska d.o.o., OIB: 29524210204, nije postupalo sukladno odredbi članka 41. Zakona o elektroničkim komunikacijama (NN br. 76/22) i članku 3. i 4. Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti mreža i usluga (NN br. 52/23) na način da nije poduzelo odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitilo sigurnost svoje mreže i usluga u odnosu na pravovremeno dokumentiranje i ažuriranje internih akata vezanih uz informacijsku sigurnost, provođenje pravovremene edukacije o podizanju svijesti o informacijskoj sigurnosti, dostavu relevantnog popisa kritičnih mrežnih komponenti i osjetljivih dijelova 5G mreže te zadovoljavajuće testiranje funkcionalnosti procesa, procedura i kontrola kontinuiteta informacijske sigurnosti.

II. Nalaže se 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 i Pravilnikom o načinu i rokovima provedbe mjera zaštite sigurnosti mreža i usluga, na način da poduzme odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga, odnosno da ukloni utvrđene nedostatke iz točke I. ovog rješenja i o navedenom dostavi dokaz inspektoru elektroničkih komunikacija Hrvatske regulatorne agencije za mrežne djelatnosti.

III. 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.

Obrazloženje

Hrvatska regulatorna agencija za mrežne djelatnosti (dalje: HAKOM) pokrenula je dana 15. lipnja 2023. godine postupak inspekcijskog nadzora nad trgovačkim društvom A1 Hrvatska d.o.o., Vrtni put 1, 10000 Zagreb, OIB:29524210204 (dalje: A1) 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

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

postupanja A1 sukladno odredbi članka 41. ZEK-a i Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti mreža i usluga (NN br. 52/23; dalje: Pravilnik) te je inspektor elektroničkih komunikacija (dalje: inspektor) obavijestio A1 da će inspekcijski pregled provesti dana 29. lipnja 2023. godine u prostorijama A1. Tijekom inspekcijskog nadzora inspektor je provjerio usklađenost informacijskog sustava A1 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 A1 dokumentirane politiku sigurnosti kao i politiku kontrole pristupa te kada su navedeni akti zadnji puta ažurirani te je utvrdio da je *Politika informacijske sigurnosti*, zadnje ažurirana […] godine, dok je *Politika kontrole logičkog pristupa,* zadnje ažurirana […]. U spomenutoj *Politici kontrole logičkog pristupa* propisano je da se periodički pregled korisničkih prava pojedinog sustava mora provesti barem jednom godišnje.

Također, inspektor je provjerio postoji li postupak kojim se osigurava da se prava pristupa korisnika ukinu nakon prestanka radnog odnosa ili da se prilagođavaju prilikom promjene te je utvrdio da postoji propisana procedura *Automatizirani proces odlaska zaposlenika* koji se inicira od strane Odjela ljudskih resursa kroz posebni sustav […], iz kojeg se informacija propagira u ostale odjele i sustave kako bi se osiguralo da se radniku koji odlazi iz kompanije pravovremeno ukinu svi pristupi na određene sustave A1, na koje je imao pristup tijekom trajanja radnog odnosa. Odjel ljudskih resursa unosi u […] sustav točan datum prestanka radnog odnosa tri radna dana prije tog datuma te se po unosu ta informacija automatski propagira prema svim članovima tima koji vode računa između ostalog i o ukidanju prava tog radnika na određene sustave. Krajnji rok za ukidanje svih prava je do ponoći zadnjeg dana radnog odnosa. Pored ovog automatiziranog procesa postoji mogućnost da rukovoditelj odjela iz kojeg radnik odlazi ukine radniku pristup i ranije. Inspektor je izvršio provjeru za zaposlenicu […] te […] čiji su radni odnosi prestali danom […]. Za zaposlenicu […] inspektor je utvrdio da je automatizirana elektronička pošta poslana […] u […] sati i da su joj ukinuta korisnička prava te je izvršena dodatna provjera u imeničkom direktoriju gdje je vidljivo da je račun onemogućen u to vrijeme. Za zaposlenicu […] inspektor je utvrdio da je poslana automatizirana elektronička pošta […]. u […], da su joj ukinuta korisnička prava te je također izvršena dodatna provjera u imeničkom direktoriju gdje je vidljivo da je račun onemogućen u to vrijeme.

Nadalje, inspektor je provjerio postoji li postupak za vlasnike imovine kojim pregledavaju redovito prava pristupa sustavima te je utvrdio da postoji *Kontrola za provođenje kvartalne provjere pregleda prava pristupa […]* te je izvršen uvid u kontrolu korisničkih prava sustava za naplatu iz lipnja 2023., kvartalnu provjeru za […] zaposlenika, gdje je utvrđeno da […] zaposlenika nemaju više potrebu imati prava pristupa za taj sustav te je u istom danu od strane odgovorne osobe kreiran zahtjev za ukidanje prava pristupa, a koji je realiziran kroz posebni "*ticketing*" sustav. Također, inspektor je utvrdio da je zaposlenik u funkciji izvršitelja kontrole prava pristupa poslao proceduru kao i rok za provođenje iste zaposleniku zaduženom za provođenje kontrole te da je kontrola izvršena u propisanom roku, odnosno unutar 7 dana.

Također, inspektor je provjerio broj zaposlenika koji su zaposleni u 2023. godini, a u odnosu na proceduru praćenja edukacija zaposlenika vezanih uz informacijsku sigurnost i postoji li testiranje zaposlenika nakon provedene edukacije te je utvrdio da A1 na dan 29. lipnja 2023. godine ima […] zaposlenika dok je ove godine zaposleno […] novih zaposlenika koji su prilikom zaposlenja dobili

popis zadataka koje moraju ispuniti prema *Onboarding planu.* Zaposlenici mogu sve zadatke jednostavno pronaći i pratiti na *[...]* koja prati zaposlenika 6 mjeseci za vrijeme trajanja probnog roka na način da kontinuirano unutar probnog roka podsjeća zaposlenika što, kada i u kojem roku mora napraviti od zadataka. Test osposobljavanja i podizanja svijesti o informacijskoj sigurnosti polaže se putem digitalne platforme […] te ukoliko zaposlenik ne napravi ili ne prođe edukaciju sustav ga upozorava na obvezu, a ako i dalje nije prošao edukaciju dobiva upozorenje od Odjela ljudskih resursa, te ako i dalje ne prođe edukaciju eskalira se na viši nivo i zaposlenik se upozorava. Inspektor je utvrdio da je za zaposlenike *[...]* u lipnju 2023. godine provedena dodatna interna edukacija „*Obuka za podizanje razine svijesti o sigurnosti*, kao i da je […] pokrenuta *Phishing kampanja* koja je obuhvatila ciljanu skupinu zaposlenika (lokalni administratori) gdje je od […] zaposlenika njih […] pristupilo poveznici iz elektroničke pošte, dok je njih […] 'upecano', odnosno isti su upisali korisničko ime i lozinku nakon pristupa poveznici. Prema navodima A1, rezultati ove kampanje prezentirati će se članu Uprave za tehniku te svih […] zaposlenika koji su se '*upecali*' moraju proći obveznu edukaciju te promijeniti lozinku. Uvidom u rezultate kampanje za nasumično odabranog […] koji se '*upecao*' upisom podataka, utvrđeno je da je isti prošao edukaciju *Podizanja svijesti informacijske sigurnosti* […] godine, kao i 2017. i 2014. godine te da zaposlenici imaju obvezu svake […] godine položiti tu edukaciju. Također, inspektor je nasumičnim odabirom zaposlenika utvrdio da je zaposlenica […], koja je zaposlena […]. godine, prošla […] godine edukaciju *Podizanja svijesti informacijske sigurnosti*, za koju je u Onboarding planu stavljen rok prvi tjedan zaposlenja, zaposlenik […] (iz IT odjela), koji je zaposlen […]. godine, istu edukaciju je prošao […]. godine, zaposlenica […] koja je zaposlena […]. godine, edukaciju je prošla […]. godine, zaposlenik […] koji je zaposlen […]. godine, edukaciju je prošao […]. godine te zaposlenik […] koji je zaposlen […]. godine, edukaciju je prošao […]. godine, a iz čega proizlazi da je od […] nasumično odabranih zaposlenika samo jedan zaposlenik prošao zahtijevanu edukaciju *Podizanja svijesti informacijske sigurnosti* u propisanom roku, odnosno u roku tjedan dana od zaposlenja, dok je jedan zaposlenik IT odjela zahtijevanu edukaciju prošao tek nakon više od […] mjeseca.

Nadalje, inspektor nije provjerio na koji način SOC nadzire 5G kritične dijelove mreže, odnosno detekciju problema vezanih uz […], iako je A1 […], sukladno članku 4. stavku 1. Pravilnika HAKOM-u dostavio popis svojih kritičnih mrežnih komponenti i osjetljivih dijelova 5G mreže te je u tom popisu naveo komponentu […] Inspektor je dodatno provjerio evidentiranje zapisa vezano uz bazne stanice te je utvrdio da je za spajanje na bazne stanice potrebno doći direktno na lokaciju te imati […], da se prati fizička sigurnost te da na nekim lokacijama postoji i video nadzor. Glede informacijske sigurnosti, inspektor je utvrdio da […] kontroliraju pokušava li se netko spojiti s neadekvatnim vjerodajnicama. Svakodnevno se pregledavaju sumnjivi događaji i dnevnički zapisi na operativnom sustavu, te se aktiviraju alarmi ukoliko se prenose […] te se zaposlenici upozoravaju ukoliko se primijeti prijenos podataka bez navođenja opravdane poslovne potrebe.

Nadalje, inspektor je provjerio postoje li dokumentirani procesi, procedure i kontrole za osiguravanje kontinuiteta informacijske sigurnosti te je utvrdio da su na snazi *Metodologija analize utjecaja na poslovanje* od […]., *Analiza utjecaja na poslovanje* […]., *Plan kontinuiteta poslovanja* […] te *Upravljanje kritičnim sustavima, […]* Inspektor je pregledao *Scenarij testiranja i testiranje plana kontinuiteta poslovanja (BCP)* […]. u kojem su provedene tri vježbe i to prva vježba uspostava rada mobilne podatkovne usluge […]., druga vježba uspostava rada mrežnih usluga […]. te treća vježba uspostava IT sustava […]. Rezultate provedenih vježbi dobio je član uprave za tehniku. Vježbe su rađene isključivo metodom *[...]*. Inspektor je pregledao i periodičko testiranje redundancije za 2022. godinu gdje su provedena […] kao i testiranje sustava za […].

Iz svega prethodno navedenog inspektor je zaključio da A1 nije u potpunosti poduzeo odgovarajuće tehničke i ustrojstvene mjere propisane člankom 3. stavom 4. Pravilnika kako bi zaštitio sigurnost svoje mreže i usluga iz sljedećih razloga. Dokumentiranje i u planiranim intervalima (jednom u 12 mjeseci) ili prilikom značajnih promjena, ažuriranje pravilnika, odnosno procedura, uputa, politika i drugih internih akata predstavlja preduvjet za osiguranje sigurnosti informacijskog sustava. A1 nije pravovremeno ažurirao dokument *Politika kontrole logičkog pristupa,* […]. Također, prilikom dolaska zaposlenika u kompaniju, isti dobivaju popis zadataka koje moraju ispuniti prema *Onboarding planu* unutar prvog tjedna zaposlenja, no prilikom provjere inspektor je nasumičnim odabirom zaposlenika utvrdio da je zaposlenica […], koja je zaposlena […], prošla 5. travnja 2023. godine edukaciju *Podizanja svijesti informacijske sigurnosti*, zaposlenik […] godine, istu edukaciju je prošao […]. godine, zaposlenica […] koja je zaposlena […]. godine, edukaciju je prošla […]. godine, zaposlenik […] koji je zaposlen […]. godine, edukaciju je prošao […]. godine te zaposlenik […] koji je zaposlen […]. godine, edukaciju je prošao […]. godine, a iz čega proizlazi da je od […] nasumično odabranih zaposlenika samo jedan zaposlenik prošao zahtijevanu edukaciju *Podizanja svijesti informacijske sigurnosti* u propisanom roku, odnosno u roku tjedan dana od zaposlenja, dok je jedan zaposlenik IT odjela zahtijevanu edukaciju prošao tek nakon više od […] mjeseca, a što ukazuje na nedostatak efikasnih mjera za realizaciju edukacije u propisanom roku, što posljedično utječe na povećanje rizika od nastanka incidenata koji mogu utjecati na sigurnost mreža i usluga A1. Nadalje, inspektor nije provjerio na koji način […], sukladno članku 4. stavku 1. Pravilnika HAKOM-u dostavio popis kritičnih mrežnih komponenti i osjetljivih dijelova 5G mreže te je u tom popisu naveo komponentu […], a iz čega proizlazi da A1 nije dostavio relevantne podatke sukladno članku 4. Pravilnika. Vezano uz testiranje funkcionalnosti procesa kontinuiteta informacijske sigurnosti, procedura i kontrola, a kako bi se osiguralo da su iste efikasne, inspektor je utvrdio da A1 provodi vježbe isključivo metodom *[…]* bez […] te da u samoj vježbi nije navedeno trajanje iste, u kojem vremenskom trenutku se koji korak odradio, već je samo navedeno da bi primjerice […]. Također, pojedina vremena za određene korake se […], a što nije zadovoljavajuće testiranje funkcionalnosti procesa kontinuiteta informacijske sigurnosti budući da samo testiranje treba biti […], a kako bi operator imao realan uvid u funkcionalnost i efikasnost procesa, kontrola i procedura.

Nastavno na prethodno navedeni zaključak, inspektor je ovim Rješenjem A1 naložio da se u roku 45 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 vezanih uz informacijsku sigurnost, provođenje pravovremene edukacije o podizanju svijesti o informacijskoj sigurnosti, dostavu relevantnog popisa kritičnih mrežnih komponenti i osjetljivih dijelova 5G mreže te zadovoljavajuće testiranje funkcionalnosti procesa, procedura i kontrola kontinuiteta informacijske sigurnosti, kao i da o navedenom dostavi dokaz inspektoru elektroničkih komunikacija Hrvatske regulatorne agencije za mrežne djelatnosti. 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 A1 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 i 110/21) za slučaj nepostupanja po ovom rješenju odgovornoj osobi izvršenika zaprijetio izricanjem novčane kazne u iznosu od 10.000 eura (slovima: deset tisuća eura) odnosno 75.345 kuna (slovima: sedamdeset pet tisuća tristo četrdeset pet 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 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. A1 Hrvatska d.o.o., Vrtni put 1, 10000 Zagreb, UP-osobnom dostavom
2. U spis