KLASA: UP/I-344-07/22-01/63
URBROJ: 376-05-22-06
Zagreb, 21. 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 nad operatorom Hrvatski Telekom d.d., Radnička cesta 21, 10000 Zagreb, OIB: 81793146560, 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 Hrvatski Telekom d.d., OIB: 81793146560, nije postupalo sukladno odredbi članka 41. Zakona o elektroničkim komunikacijama (NN br. 76/22).

II. Utvrđuje se da trgovačko društvo Hrvatski Telekom d.d., OIB: 81793146560, nije poduzelo odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga u odnosu na pravovremeno dokumentiranje i ažuriranje internih akata, deaktiviranje prava i sredstva fizičkog pristupa kao i pristupa podacima zaposleniku na dan prestanka ugovora o radu, pravovremeni pregled i ažuriranje korisničkih prava, provođenje pravovremenih, adekvatnih edukacija o podizanju svijesti o informacijskoj sigurnosti te pravovremeno testiranje funkcionalnosti procesa, procedura i kontrola kontinuiteta informacijske sigurnosti.

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), 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 75.345,00 kn (slovima: sedamdesetpet tisuća tristočetrdesetpet

kuna) / 10.000 eura[1] (slovima: deset tisuća eura). 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 Hrvatski Telekom d.d., Radnička cesta 21, OIB: 81793146560 (dalje: HT) 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 HT-a sukladno odredbi članka 41. ZEK-a i Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/2021) (dalje: Pravilnik) te je inspektor elektroničkih komunikacija (dalje: inspektor) obavijestio HT da će inspekcijski pregled provesti dana 17. studenog 2022. godine u prostorijama HT-a.

Tijekom inspekcijskog nadzora inspektor je provjerio usklađenost informacijskog sustava HT-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 HT dokumentiranu politiku kontrole pristupa, kada je zadnji puta ista ažurirana, tko ju je napisao, pregledao i odobrio te koliko često se pregledava, te je utvrdio da je donesena politika na razini […] pod nazivom […], zadnje ažurirana […] godine, odobrena od strane Uprave HT-a te u dokumentu nije navedeno tko je isti izradio, a tko pregledao.

Također, inspektor je provjerio postoji li postupak kojim se osigurava da se prava pristupa korisnika ukinu nakon prestanka radnog odnosa, ugovora ili da se prilagođavaju prilikom promjene te je utvrdio da prvo zaposlenik šalje zahtjev za raskid radnog odnosa nadređenom koji to prijavljuje odjelu HR (ljudskih potencijala) koji to zatim upisuje u […]. […] šalje automatsku poruku na […] (platforma za […]) te se tu pokreće proces ukidanja svih prava. Utvrđeno je da je donesen dokument […] u kojem je u članku […] propisano što je potrebno poduzeti kada zaposlenik odlazi iz kompanije, odnosno da mu se prava i sredstva fizičkog pristupa, kao i pristup podacima moraju deaktivirati na dan odlaska iz kompanije. Također, na intranetu postoje kratke upute o prestanku radnog odnosa pod nazivom […]. Inspektor je u sustavu nasumično odabrao dva zaposlenika koji su u zadnja tri mjeseca imali prestanak ugovora o radu i to: […], koja je […] godine mailom poslala zahtjev za raskid ugovora, datum zaprimanja potpisanog sporazuma u sustav […] bio je […] godine, dok je […] nastupio prestanak ugovora o radu, te […], čiji je zahtjev za raskid ugovora zaprimljen […] godine, datum zaprimanja potpisanog sporazuma u sustav […] bio je […] godine, dok je datum prestanka ugovora o radu bio […] godine. Za prvu djelatnicu […] godine odmah iza […] ukinuta su sva prava pristupa u sustavu, dok je u […] sati obrisan i njen korisnički profil na domeni kao i njen pretinac elektroničke pošte. Za drugu zaposlenicu sva prava pristupa ukinuta su […] godine, odnosno […].

[1] Preračunato po fiksnom tečaju konverzije (1 EUR=7.53450 kn)

Nadalje, inspektor je provjerio postoji li postupak za vlasnike imovine kojim pregledavaju redovito prava pristupa sustavima te je utvrdio da postoji interni sustav kontrola ([…]) te da svaka aplikacija ima svog vlasnika. Zadnja kontrola prava pristupa za kritične sustave provedena je […] godine za ukupno […] korisničkih računa, od kojih je ukinuto […] računa, a što je navedeno u tablici […], koja sadrži podatke o provjerama dodijeljenih prava pristupa zaposlenika, odnosno pravima pristupa koja su trebala prethodno biti ukinuta iz razloga promjene posla, radnog mjesta, odjela i sličnih razloga.

Također, inspektor je provjerio broj zaposlenika koji su zaposleni 2022. godine, proceduru praćenja edukacija zaposlenika vezanih uz informacijsku sigurnost i postoji li testiranje zaposlenika nakon provedene edukacije te je utvrdio da novi zaposlenici prilikom zaposlenja dobiju pristup […] aplikaciji […] u kojoj su navedene upute o […], […] i […], odnosno o edukacijama koje su obavezne za zaposlenika i njegovo radno mjesto. Nakon provedene edukacije, nadređeni, kao i zaposlenik, dobivaju potvrdu da je edukacija položena. Edukacija je provedena na način da zaposlenik dobije sve potrebne informacije te nakon što ih pročita, rješava test, a da bi se edukacija prošla svi odgovori moraju biti točni. U navedenoj aplikaciji propisana je obveza testiranja i edukacija zaposlenika vezano uz […], […] i […], uz napomenu da su svi zaposlenici obvezni završiti […] edukaciju o zaštiti osobnih podataka i privatnosti prije pristupanja obradi osobnih podataka, uz molbu da se tijekom svog prvog mjeseca (čim se zaposleniku dodijeli […] račun elektroničkom poštom) pristupi edukaciji. Ukupan broj zaposlenika na dan 17. studenog 2022. godine iznosio je […]. U 2022. godini zaposleno je […], a prekid ugovora o radu imalo je […] zaposlenika. Inspektor je nasumičnim odabirom odabrao dva zaposlenika koji su započeli rad u rujnu 2022. godine i to […] ([…]) i […] ([…]). Za oba zaposlenika je ugovor o radu započeo 1. rujna 2022. godine te je za oba zaposlenika utvrđeno da nisu prošli […] obveznu edukaciju navedenu u aplikaciji […]. Nazočne osobe navele su da su i nadređeni i sam zaposlenik dobili „alarm“ da edukacija nije obavljena u roku mjesec dana te da će provjeriti zašto zaposlenici nisu završili navedenu […] edukaciju te će svoje očitovanje dostaviti naknadno, u roku od osam (8) dana od dana izvršenog inspekcijskog pregleda.

Nadalje, inspektor je provjerio postoje li dokumentirani procesi, procedure i kontrole za osiguravanje kontinuiteta informacijske sigurnosti, odnosno postoje li propisani plan, odgovor, procedure i vrijeme oporavka kao i kompenzacijske kontrole koje se koriste kada propisane kontrole informacijske sigurnosti ne mogu biti održane tijekom nepovoljne situacije. Inspektor je utvrdio da je na snazi […] od […] godine u kojoj je definirana organizacija kriznog menadžmenta te ažurirani […] (iz […] godine), a u kojem su definirani svi procesi postupanja i upravljanja krizama kao i uloge, odgovornosti i obveze. Također, utvrđeno je da su doneseni: […] (iz […] godine), […], zadnje ažurirani […] godine. Nadalje, vezano uz kompenzacijske kontrole koje koriste za kontrole informacijske sigurnosti koje ne mogu biti održane tijekom nepovoljne situacije, nazočne osobe zamolile su inspektora da im dodijeli rok za dostavu prethodno spomenutoga, a što je inspektor uvažio te im je odredio rok za dostavu dokumentacije od osam (8) dana od dana izvršenog inspekcijskog pregleda. Inspektor je pregledao i dokument […] koji se odnosi na analizu utjecaja poslovanja vezano uz […] (od […] godine).

Također, inspektor je iz sustava upravljanja incidentima […] koji služi za kontrolu te sadrži procedure upravljanja incidenata tijekom nepovoljnih situacija nasumično odabrao jednu proceduru za postupanje prilikom poteškoća i to za nepokretnu mrežu te izvršio uvid u […], zadnje ažuriranog […] godine, a u kojem je propisan plan upravljanja kontinuitetom poslovanja kako bi se osigurala neprekinutost poslovanja u slučajevima prekida rada […] sustava koje koriste zaposlenici koji rade kao […] i zaposlenici iz radnih jedinica koje imaju […], ili su podrška u stvarnom vremenu odjelima koji su u […].

Nadalje, inspektor je provjerio postoje li vježbe i testiranje funkcionalnosti procesa kontinuiteta informacijske sigurnosti, procedura i kontrola kako bi se osiguralo da su iste efikasne te je nasumičnim odabirom izvještaja testiranja odabrao izvještaj […] ([…]*).* Utvrdio je da je zadnje testiranje provedeno u […] godine te je u izvještaju navedeno nekoliko radnji koje je potrebno poduzeti i to: da je potrebno provoditi test krizne procedure svakih […], da bi članovi upravljačkog kriznog tima trebali, osim što prime […], biti kontaktirani i putem […], da je potrebno zaprimiti […] ([…]) od strane kriznog tehničkog tima unutar […], barem na početku procesa jer je isto ključno za odluku o komunikacijskoj strategiji, da je potrebno izvršiti provjeru […] iz […] svakih […] i […], da je potrebno napraviti analizu *case–by-case* (od slučaja do slučaja) […] i […] statusa […] tijekom testiranja, da je potrebno izvršiti redovite provjere veza na […] lokacijama ([…] na glavnoj […] lokaciji, ostale lokacije […]) te da je potrebno poslati informaciju prema korisnicima […] uređaja da uređaji moraju biti uključeni tijekom krize. Rok za implementaciju navedenih radnji postavljen je u periodu od […] do […] godine. Nazočne osobe zamolile su inspektora da im dodijeli rok za očitovanje na predmetno izvješće te im je inspektor dodijelio rok za očitovanje od osam (8) dana od dana izvršenog inspekcijskog pregleda.

Dana 25. studenog 2022. godine HT se očitovao na nalaz inspekcijskog pregleda vezano uz […] edukaciju o informacijskoj sigurnosti na način da je analizom utvrdio da zaposlenici […] i […] nisu dobili poziv za edukaciju u sklopu […] jer je sustav kontrole nedostatan te da je potrebno uvesti redovitu kvartalnu provjeru o prolaznosti radnika HT-a vezano uz obaveznu edukaciju, dok bi sama kontrola uključivala usporedbu popisa zaposlenika koji su ušli u kompaniju u određenom kvartalu s popisom zaposlenika koji su prošli obaveznu edukaciju, kao i efikasnu proceduru eskalacije za zaposlenike koji edukaciju nisu završili u roku. Također, HT je napomenuo da u […] planira edukaciju iz područja […] poslati na sve zaposlenike koji je nisu imali u […] ili […] godini, s rokom ispunjenja od […] te će na taj način i […] i […] biti obuhvaćeni. Nadalje, vezano uz kompenzacijske kontrole, HT se očitovao da ima odgovarajuću upravljačku strukturu i potrebnu radnu snagu s ovlastima, iskustvom i kompetencijom za planiranje, ublažavanje i odgovor na neželjene i krizne događaje. Jednako tako, da ima imenovane osobe za upravljanje incidentima i informacijskom sigurnošću, s definiranom potrebnom odgovornošću, ovlastima i kompetencijama te da je izradio, odobrio i dokumentirao planove za nastavak kontinuiteta poslovanja, procedure odgovora i oporavka, koji opisuju kako HT upravlja neželjenim događajima i održava razinu sigurnosti informacija. U odnosu na kompenzacijske kontrole za kontrole informacijske sigurnosti koje ne mogu biti održane tijekom nepovoljne situacije, HT je naveo da su one najvećim dijelom pokrivene […] jer su sustavi/procesi i procedure iz područja informacijske sigurnosti istovremeno ključni i za pružanje usluga korisnicima. Također, HT je dostavio i izvještaj s testiranja kritičnih IT/NT sustava u […] godini *(*[…]*),* aktivnosti i testiranja iz područja zaštite na radu i zaštite od požara u razdoblju Q4/2021 - Q3/2022, te provjeru usklađenosti implementiranih mjera fizičke sigurnosti s Deutsche Telekom-ovim certifikatima na lokacijama […] i […], u 2022. godini. Nadalje, HT se očitovao i na izvješće o testiranju krizne procedure […] *(*[…]*)* navodeći da su, umjesto testiranja, održane edukacije po kriznim timovima putem MS Teamsa, testiranje alternativnih kriznih priključaka ([…] i […]) u razdoblju od […] do […] te da je ponovno testiranje krizne procedure planirano za […] godine, dok je ažuriranje krizne procedure i njegovo odobrenje od strane Uprave planirano za […] godine. Nadalje, HT je naveo kako će članovi svih kriznih timova, osim […], ako se ne […], biti pozvani dostupnim […] te će isto biti uvršteno i u ažuriranje krizne procedure u […] godine. Također, u

brošuri za […] (slide […]), kratkim i jasnim uputama za postupanje članovima […], a koja sadrži informacije tko, kada, kako i što radi tijekom […] i dostupna je svim članovima […] na *share pointu* (zajedničkoj točki) za […], sadržana je informacija o […] ([…]) svakih […] (zadnja verzija […]). Vezano uz potrebu izvršenja provjere popisa primatelja iz […] svakih […] i prije […], HT se očitovao da je zadnja revizija napravljena […], od strane partnera […], koji održava sustav […], dok se na dio vezan uz analizu case–by-case (od slučaja do slučaja) […] i […] statusa […] tijekom testiranja očitovao navodeći da su članovi kriznog managementa pojedinačno kontaktirani u […] godine te da je testiranje […] za sve članove kriznog managementa napravljeno u razdoblju od […] do […]. Nadalje, HT se očitovao i na potrebu redovite provjere veza na […] lokacijama ([…] na glavnoj […] lokaciji, ostale lokacije […]) navodeći da je s društvom […] […] sklopljen novi […] za […] lokacije ([…]) te da usluge uključuju pristup na Internet putem optičkog voda i *voice* (govorne) priključke. Priključci su testirani […] od strane zaposlenika Odsjeka za […] i Odsjeka za […] ([…]). Vezano uz slanje informacije prema korisnicima […] mrežnih uređaja da uređaji moraju biti uključeni tijekom krize HT je u svom očitovanju pojasnio da je […] komunicirano članovima kojima su […] prilikom […].

Iz svega prethodno navedenog inspektor je zaključio da HT nije u potpunosti poduzeo odgovarajuće tehničke i ustrojstvene mjere 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. HT nije pravovremeno ažurirao dokumente: […] u kojem nije niti navedeno tko je isti izradio, a tko pregledao, zatim dokumente […], još od […] godine, dokument […] koji se odnosi na analizu utjecaja poslovanja vezano uz govornu uslugu u fiksnoj mreži te […]. Također, prilikom odlaska zaposlenika iz kompanije, odnosno prestanka ugovora o radu, zaposlenicima se prava i sredstva fizičkog pristupa kao i pristup podacima moraju deaktivirati na dan odlaska iz kompanije, a što HT nije učinio za provjerene zaposlenike […] i […], odnosno zaposlenicama su sva prava pristupa ukinuta tek […], a što je u suprotnosti s HT-ovim dokumentom […] čl. […]. Nadalje, prilikom provjere pregleda prava pristupa sustavima inspektor je utvrdio da je zadnja sveobuhvatna kontrola prava pristupa […] za kritične sustave provedena […] godine za ukupno […] korisničkih računa, od kojih je ukinuto […] računa, a što po mišljenju inspektora ukazuje na nedostatnost pregleda korisničkih prava pravovremeno, odnosno prilikom bilo kakvih promjena, uloga, odjela i slično, a što je također u suprotnosti sa zahtjevima nacionalnih i međunarodnih standarda za očuvanje informacijske sigurnosti. Prilikom provjere edukacije zaposlenika o informacijskoj sigurnosti inspektor je nasumičnim odabirom utvrdio da odabrana dva zaposlenika koji su započeli rad 1. rujna 2022. godine i to […] ([…]) i […] ([…]) nisu prošli […] obveznu edukaciju navedenu u aplikaciji […] iako su i nadređeni i sam zaposlenik dobili „alarm“ da edukacija nije obavljena u roku […] jer je sustav kontrole nedostatan što je i sam HT potvrdio u svom očitovanju dana 25. studenog 2022., a što povećava rizik od nastanka incidenata koji mogu utjecati na sigurnost i cjelovitost mreža i usluga HT-a. Vezano uz testiranje funkcionalnosti procesa kontinuiteta informacijske sigurnosti, procedura i kontrola, a kako bi se osiguralo da su iste efikasne, inspektor je nasumičnim odabirom izvještaja testiranja utvrdio da je izvještaj […] ([…]) iz […] godine, odnosno da nije provedeno novo testiranje krizne procedure unutar 12 mjeseci, a što je u suprotnosti sa zahtjevima nacionalnih i međunarodnih standarda za očuvanje informacijske sigurnosti. Također, inspektor smatra da provođenje edukacije po kriznim timovima putem MS Teamsa nije adekvatna zamjena za samo testiranje već preduvjet provođenja testiranja.

Nastavno na prethodno navedeni zaključak, inspektor je ovim Rješenjem HT-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 vezanih uz informacijsku sigurnost, deaktiviranje prava i sredstva fizičkog pristupa kao i ukidanje prava pristupa podacima zaposlenika na dan prestanka ugovora o radu, pravovremeni pregled i ažuriranje korisničkih prava, provođenje pravovremene, adekvatne edukacije o podizanju svijesti o informacijskoj sigurnosti te pravovremeno 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 HT 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 75.345,00 kn (slovima: sedamdesetpet tisuća tristočetrdesetpet kuna)/ 10.000 eura (slovima: deset tisuća eura), preračunato po fiksnom tečaju konverzije 1 EUR = 7,53450 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. Hrvatski Telekom d.d., Radnička cesta 21, 10000 Zagreb, UP-osobnom dostavom
2. U spis