KLASA: UP/I-344-07/23-01/95
URBROJ: 376-05-23-05
Zagreb, 17. siječnja 2024.

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 upravljanje imovinom u skladu s važećom informacijskom klasifikacijskom shemom, pravovremeno otklanjanje tehničkih ranjivosti, neprovođenje PSA (P*rivacy and Security Assessment*) jednom u 3 godine za kritične sustave i sustave koji imaju sigurnosnu ili podatkovnu važnost, čak i u slučaju da nije bilo izmjena na sustavu te u odnosu na nedostatak pridruživanja vrijednosti i RTO-a (R*ecovery Time Objective*) pojedinoj imovini.

III. Nalaže se društvu iz točke I. ovog rješenja da u roku 30 dana od primitka ovog rješenja poduzme odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga, odnosno uskladi svoje postupanje 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) te da ukloni utvrđene nedostatke 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). U slučaju daljnjeg neispunjavanja obveze, izreći će se druga, veća novčana kazna.

Obrazloženje

Hrvatska regulatorna agencija za mrežne djelatnosti (dalje: HAKOM) pokrenula je dana 19. listopada 2023. 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 Pravilniku 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 HT da će inspekcijski pregled provesti dana 7. studenog 2023. 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 klasifikaciju informacija i korištenje kriptografskih kontrola za zaštitu informacija, odnosno provjeru ima li HT dokumentiranu politiku ili proceduru upravljanja imovinom u skladu s informacijskom klasifikacijskom shemom koju je implementirao te politiku korištenja kriptografskih kontrola za zaštitu informacija. Inspektor je u postupku utvrdio da je HT usvojio dokument [] koji propisuje na koji način zaposlenici i poslovne jedinice moraju klasificirati i, ako je potrebno, označavati osobne podatke i informacije u svrhu zaštite podataka, a koji je HT nakon izvršenog inspekcijskog pregleda ažurirao i dostavio inspektoru dana 15. studenog 2023. U dokumentu je propisano da postoje [] razine klasifikacije: [] te je za razinu [] propisano da podaci moraju biti posebno zaštićeni. Inspektor je, nasumičnim odabirom, pregledao tri primjera slanja povjerljivih informacija, odnosno informacija koji spadaju u kategoriju [ ] i to slanje tablica „Analiza brzina širokopojasnog pristupa internetu“ koje HAKOM redovito zaprima. Zadnji puta je HAKOM zaprimio povjerljive podatke 13. studenog 2023. putem elektroničke pošte bez oznake povjerljivo. Dodatno, pregledana je i obavijest o izmjenama ponuda za korisnike bonova HT-a u pokretnoj elektroničkoj komunikacijskoj mreži gdje su povjerljivi podaci slani dana 31. listopada 2023. s oznakom poslovna tajna, ali elektronička pošta nije bila dodatno zaštićena. Isto tako, pregledano je očitovanje na dopis Agencije za zaštitu osobnih podataka od 13. listopada 2023. gdje je datoteka s osobnim podacima zaštićena lozinkom. Pregledan je i dokument pod nazivom […] u kojem su navedeni zahtjevi za kriptografske algoritme i sigurnosne protokole. Inspektor je nasumičnim odabirom izvršio provjeru na javnom web portalu gdje https konekcija koristi preporučeni TLS 1.3. uz algoritam [] mehanizam za razmjenu ključa te na intranetu, gdje se koristi preporučeni algoritam [], a što je sukladno dokumentu [].

Također, inspektor je provjerio postoji li proces za praćenje, testiranje i ocjenu tehničkih ranjivosti kao i koje su mjere poduzete za njihovo pravovremeno uklanjanje te je utvrdio da je donesen dokument pod nazivom [] koji propisuje minimalni set sigurnosnih mjera za sustave, odnosno kojim je propisano da se mora provoditi praćenje tehničkih ranjivosti. Sam proces praćenja tehničkih ranjivosti opisan je u dokumentu []. Pregledan je i izvještaj [] iz rujna 2023. u kojem su navedene sve ranjivosti na razini EU DT-a, a koji služi za izvještavanje višeg rukovodstva o stanju kibernetičke sigurnosti unutar DT grupe te za praćenje duljine prisutnosti određene ranjivosti. Također, pregledan

je i tjedni izvještaj sigurnosnih ranjivosti javnih servisa od 6. studenog 2023. u kojem su navedene 3 pronađene ranjivosti razine 4 (visoka razina). Ranjivost - [] označena je procijenjenom razinom ranjivosti CVSS-om (*Comon Vulnerability Scoring System*) 8.1 te je ranjivost privremeno riješena taj dan, no primijećeno je da je ista prvi puta uočena 29. rujna 2023., eskalirana 2. listopada 2023. te ponovno 16. listopada 2023., te da krajnji rezultat ukazuje na lažno pozitivnu ranjivost koja je trajno uklonjena 6. studenog 2023. Za druge dvije ranjivosti - [] utvrđeno je da je ista još u postupku rješavanja te da je ranjivost prvotno detektirana 28. rujna 2023. Također, preuzet je i izvještaj sigurnosnih ranjivosti javnih servisa od 1. studenog 2023. u kojem je uočeno 7 ranjivosti razine 4, od kojih su se 4 otklonile, a 3 su uočene i u novom izvještaju 6. studenog 2023. Za sustav naplate nije rađen penetracijski test niti procjena utjecaja na privatnost i sigurnost, tzv. PSA (*privacy and security assessment*) od 2018. te je isto naznačeno u internoj tablici rizika. Pregledan je i dokument [] gdje je propisano da je za kritične sustave i sustave koji imaju sigurnosnu ili podatkovnu važnost, PSA potrebno provesti jednom u 3 godine čak i u slučaju da nije bilo izmjena na sustavu.

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. U tu svrhu, inspektor je pregledao [] te je nasumično odabrao imovinu [] za koju je ustanovio da nije napravljena procjena rizika kao i da nije određeno vrijeme oporavka, tzv. RTO (*Recovery Time Objective*). Pregledana je i [], kao i [] u kojem je provjeren status testiranja []. Utvrđeno je da su provedena 3 testiranja i to: 24. siječnja 2023. [] u Zagrebu, 20. veljače 2023. [] u Zagrebu i 6. ožujka 2023. [] u Rijeci te da su redundantne lokacije Rijeka i Split preuzele predviđen promet. Također, pregledan je i test [] te je utvrđeno da su redundantne lokacije Rijeka i Split preuzele promet na period od 4 mjeseca, koliko je trajala nadogradnja []. Pregledan je plan opravka od katastrofe za Data Centar - [] u kojem je opisan proces plana oporavka za sve *data* centre, no samo testiranje rušenja pojedinog cijelog *data* centra se ne provodi.

Iz svega prethodno navedenog inspektor je zaključio da HT nije postupao sukladno Pravilniku te da nije u potpunosti poduzeo odgovarajuće tehničke i ustrojstvene mjere kako bi zaštitio sigurnost svoje mreže i usluga budući da nepostupanje HT sukladno dokumentima koje je sam usvojio, a vezano uz informacijsku sigurnost, predstavlja znatan rizik u očuvanju informacijske sigurnosti i nije u skladu s važećim međunarodnim standardima informacijske sigurnosti. Nastavno na prethodno navedeno, HT nije upravljao imovinom u skladu s propisanom informacijskom klasifikacijskom shemom, u ovom slučaju u skladu s informacijskom klasifikacijskom shemom iz važećeg dokumenta [] koji propisuje na koji način zaposlenici i poslovne jedinice moraju klasificirati i, ako je potrebno, označavati osobne podatke i informacije u svrhu zaštite podataka. Za razinu [] dokumentom je propisano da podaci moraju biti posebno zaštićeni, a što je inspektor utvrdio da nije bio slučaj prilikom pregleda slanja povjerljivih podataka unutar tablice „Analiza brzina širokopojasnog pristupa internetu“ koju je HAKOM zaprimio 13. listopada 2023. putem elektroničke pošte bez oznake povjerljivo i bez posebne zaštite podataka kao i kod zaprimanja obavijesti o izmjenama ponuda za korisnike bonova HT-a u pokretnoj elektroničkoj komunikacijskoj mreži gdje su povjerljivi podaci slani dana 31. listopada 2023. s oznakom poslovna tajna, ali podaci nisu bili dodatno zaštićeni. Nadalje, prilikom pregleda tjednog izvještaja sigurnosnih ranjivosti javnih servisa od 6. studenog 2023. u kojem su navedene 3 pronađene ranjivosti razine 4 (visoka razina), inspektor je utvrdio da je ranjivost [] označena s procijenjenom razinom ranjivosti CVSS-om (*Comon Vulnerability Scoring System*) 8.1, prvi puta uočena 29. rujna 2023., eskalirana 2. listopada 2023. te ponovno 16. listopada 2023., te da krajnji rezultat ukazuje na lažno pozitivnu ranjivost koja je trajno uklonjena tek 6. studenog 2023., dok je za druge dvije ranjivosti [] utvrđeno da su još u postupku rješavanja te da je ranjivost prvotno detektirana 28. rujna 2023. Iz prethodno navedenog inspektor zaključuje da se

ranjivosti ne otklanjaju pravovremenou skladu s propisanim dokumentom [] koji propisuje predviđena vremena otklona ranjivosti za pojedine razine i to za razine [], za implementaciju privremenog rješenja, do 14 kalendarskih dana, a za implementaciju službenog rješenja do 30 kalendarskih dana. Također, inspektor je utvrdio da za sustav naplate nije rađen penetracijski test niti procjena utjecaja na privatnost i sigurnost, tzv. PSA (*privacy and security assessment*) od 2018. iako je sukladno dokumentu [] propisano da je za kritične sustave i sustave koji imaju sigurnosnu ili podatkovnu važnost, PSA potrebno provesti jednom u 3 godine, čak i u slučaju da nije bilo izmjena na sustavu. Nadalje, prilikom pregleda dokumenta [] inspektor je utvrdio da HT nije pridružio pojedinoj imovini vrijednost kao ni vrijeme oporavka, tzv. RTO (*recovery time objective*), a što upućuje na zaključak da HT provodi nedovoljno temeljito procjenu rizika, a što predstavlja vrlo važan dio osiguranja sigurnosti mreža i usluga.

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 upravljanje imovinom u skladu s važećom informacijskom klasifikacijskom shemom, pravovremenim otklanjanjem tehničkih ranjivosti, provođenjem PSA (*Privacy and Security Assessment*) jednom u 3 godine za kritične sustave i sustave koji imaju sigurnosnu ili podatkovnu važnost, čak i u slučaju da nije bilo izmjena na sustavu, pridruživanje vrijednosti i RTO-a (R*ecovery Time Objective*) pojedinoj imovini, 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 10.000 eura (slovima: deset tisuća eura), 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.

Dostaviti:
1. Hrvatski Telekom d.d., Radnička cesta 21, 10000 Zagreb, UP-osobnom dostavom
2. 2. U spis

INSPEKTOR ELEKTRONIČKIH KOMUNIKACIJA

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