KLASA: UP/I-344-07/22-01/15
URBROJ: 376-05-22-10
Zagreb, 20. lipnja 2022.

Na temelju članka 12. stavka 1. točke 14. i članka 111. stavka 1. i 2. Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17), te članka 96. Zakona o općem upravnom postupku (NN br. 47/09), u inspekcijskom postupku pokrenutom po službenoj dužnosti protiv operatora A1 Hrvatska d.o.o., Vrtni put 1, 10000 Zagreb, OIB: 29524210204, radi kršenja odredbi članka 99. i 99.a Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17) te odredbi članka 3. i 6. Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21), inspektor elektroničkih komunikacija Hrvatske regulatorne agencije za mrežne djelatnosti donosi

RJEŠENJE

I. Utvrđuje se da trgovačko društvo A1 Hrvatska d.o.o., Vrtni put 1, 10000 Zagreb, OIB: 29524210204, prilikom nastanka sigurnosnog incidenta nije postupilo u skladu s člankom 6. stavak 1. i stavak 3. Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21), a koji se odnosi na obvezu operatora da obavijest o sigurnosnim incidentima dostavi Agenciji bez odgode, čim su podaci dostupni, u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, u roku od najviše 1 sat nakon otklanjanja sigurnosnog incidenta te u roku od najviše 20 dana od dana otklanjanja sigurnosnog incidenta, upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku elektroničkim putem na adresu elektroničke pošte: incidenti@hakom.hr ili na drugi prikladan način.

II. Utvrđuje se da trgovačko društvo A1 Hrvatska d.o.o., Vrtni put 1, 10000 Zagreb, OIB: 29524210204, nije postupilo u skladu s člankom 3. stavka 1. Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21), a koji se odnosi na obvezu operatora da poduzima odgovarajuće tehničke i ustrojstvene mjere, uključujući šifriranje kada je primjereno, radi zaštite sigurnosti i cjelovitosti svojih mreža i usluga te sprječavanja i umanjenja utjecaja sigurnosnih incidenata na korisnike usluga i međupovezane elektroničke komunikacijske mreže i usluge, pri čemu poduzete mjere moraju osigurati razinu sigurnosti koja odgovara postojećoj razini opasnosti za sigurnost mreže i usluga, a zbog čega je posljedično dovelo do pojave sigurnosnog incidenta.

III. Nalaže se društvu iz točke I. ovog rješenja da odmah po primitku ovog rješenja poduzme odgovarajuće tehničke i ustrojstvene mjere radi zaštite sigurnosti i cjelovitosti svojih mreža i usluga te sprječavanja i umanjenja utjecaja sigurnosnih incidenata na korisnike usluga te da primjenjuje procedure kojima će osigurati detektiranje i pravovremeno prijavljivanje sigurnosnih incidenata sukladno Zakonu o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17) i Pravilniku o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21).

IV. U slučaju nepostupanja po ovom rješenju, odgovornoj osobi izvršenika, izreći će se novčana kazna u iznosu od 75.000,00 kn (slovima: sedamdesetpet 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 22. veljače 2022. godine postupak inspekcijskog nadzora nad trgovačkim društvom A1 Hrvatska d.o.o., Vrtni put 1, 10000 Zagreb, OIB: 29524210204 (dalje: A1) sukladno članku 12. stavku 1. točki 14., članku 15., a temeljem članka 111. i 112. Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17, dalje: ZEK), u svezi utvrđivanja postupanja A1 sukladno odredbama članka 99. i 99.a ZEK-a te odredbe članka 3., 6., 7. i 8. Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 112/21, dalje: Pravilnik).

Dana 9. veljače 2022. A1 je u 12:07 obavijestio HAKOM putem elektroničke pošte na adresu incidenti@hakom.hr o incidentu koji je prema navodima A1 uzrokovan neovlaštenim pristupom A1 sustavu uz prijetnju objavljivanja neovlašteno stečenih osobnih podataka značajnog broja korisnika A1 (dalje: sigurnosni incident). Istoga dana, u 14:09 putem elektroničke pošte na adresu zastita.osobnipodaci@hakom.hr A1 je obavijestio HAKOM i o povredi osobnih podataka korisnika.

Nakon inicijalne prijave povrede osobnih podataka, A1 je dostavio i obavijest o javnim objavama kojima je krajnje korisnike obavijestio o incidentu. A1 je također zatražio mišljenje HAKOM-a o obvezi dodatnog obavještavanja korisnika. Istoga dana, 9. veljače 2022. u 16:03 HAKOM je poslao mišljenje prema kojem je A1, sukladno članku 99.a stavak 2. ZEK-a obvezan obavijestiti krajnje korisnike o povredi. Sukladno mišljenju HAKOM-a, A1 je dana 9. veljače 20222. u 17:32 i dodatno 10. veljače 2022. obavijestio HAKOM o sadržaju obavijesti koje je krajnjim korisnicima uputio SMS porukom i elektroničkom poštom.
U odnosu na prijavljeni sigurnosni incident, inspektor elektroničkih komunikacija HAKOM-a je pokrenuo inspekcijski nadzor radi utvrđivanja činjeničnog stanja te naložio A1 da u roku osam (8) dana od dana dostave dopisa dostavi očitovanje na okolnosti navedene u dopisu, posebice u odnosu na pravovremenu prijavu sigurnosnog incidenta sukladno Pravilniku, poduzimanju odgovarajućih sigurnosnih mjera, kao i okolnostima nastanka sigurnosnog incidenta. Pored očitovanja na konkretno postavljena pitanja, HAKOM je zatražio dostavljanje podataka i relevantnih dokaza.

Dana 8. ožujka 2022. godine HAKOM je zaprimio očitovanje A1 u kojem A1 navodi da je u potpunosti svjestan kriterija za izvješćivanje HAKOM-a o sigurnosnim incidentima iz Dodatka 2. Pravilnika, kao i o obvezi provjere ispunjavanja Kvantitativnih i Kvalitativnih kriterija iz navedenog Dodatka, pri tom navodi da strogo slijedi odredbu članka 1. Pravilnika koja utvrđuje da se obveze Pravilnika o izvješćivanju HAKOM-a odnose na povrede sigurnosti i/ili gubitka cjelovitosti od značajnijeg utjecaja na rad A1 mreža i obavljanje usluga, kao što i slijedi iz odredbe članka 6. stavka 1. Pravilnika kojim se utvrđuje obveza izvješćivanja HAKOM-a o sigurnosnom incidentu koji je značajnije utjecao na rad mreža i/ili usluga. Pojašnjava da je ista obveza jasno utvrđena i u članku 99. stavku 7. ZEK-a na način da su operatori javnih komunikacijskih mreža i operatori javno dostupnih elektroničkih komunikacijskih usluga dužni bez odgode izvijestiti Agenciju pisanim putem o povredi sigurnosti ili gubitku cjelovitosti od značajnog utjecaja na rad njihovih mreža ili obavljanje njihovih usluga te iako je postojala visoka vjerojatnost da se u A1 mreži dogodio sigurnosni incident kojim su ugroženi osobni podaci korisnika, bilo je razvidno da takvi događaji nisu utjecali na rad A1 mreže ili pružanje usluga u smislu gore navedenih propisa te bez obzira na izostanak ispunjenja Kvantitativnih i Kvalitativnih kriterija iz Dodatka 2 Pravilnika i bez obzira na činjenicu da predmetni sigurnosni incident ne predstavlja povredu sigurnosti ili gubitak cjelovitosti od značajnog utjecaja na rad A1 mreža ili obavljanje usluga, A1 je uzimajući u obzir načelo transparentnosti te potrebu uske suradnje s HAKOM-om kod ovakvih događaja, obavijestio HAKOM o povredi osobnih podataka i sigurnosnog incidenta dana 09.02.2022. u 12:07 putem elektroničke pošte na adresu incidenti@hakom.hr te dana 09.02.2022. u 14:09 putem elektroničke pošte na adresu zastita.osobnipodaci@hakom.hr.

[redacted]

A1 osobito ističe kako sve relevantne okolnosti nisu ukazivale na postojanje povrede sigurnosti ili gubitka cjelovitosti, odnosno, sigurnosnog incidenta koji bi značajnije utjecao na rad mreža i/ili usluga u smislu članka 99. ZEK-a i članka 6. Pravilnika, a kako je naknadno potvrđeno kroz detaljne analize. U odnosu na rokove iz Pravilnika, prema kojima postoji obveza prijave sigurnosnog incidenta u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, odnosno isteka minimalnog trajanja sigurnosnog incidenta, A1 ukazuje kako isti rok nije primjeren i primjenjiv s obzirom na sve okolnosti ovoga slučaja, a osobito činjenicu da se ne radi o sigurnosnom incidentu u smislu Pravilnika, odnosno da je razvidno da niti Kvantitativni kriteriji niti Kvalitativni kriteriji za izvješćivanje iz Dodatka 2. Pravilnika nisu bili ispunjeni, te nije postojala obveza dostavljanja obavijesti o incidentu na način i u rokovima propisanim Pravilnikom. Nadalje, A1 navodi da je razvidno kako s obzirom na karakter sigurnosnog incidenta, uz uvažavanje svih činjenica i utvrđenih okolnosti, sigurnosni incident nema svoje jednoznačno vrijeme trajanja, ali ističe da su s danom 11.02.2022. godine u cijelosti uklonjeni svi eventualni rizici za potencijalno izložene korisnike MOZAIK tarife A1, uklanjanjem javno objavljenih osobnih podataka korisnika na javnosti nepoznatim internetskim stranicama. Također, A1 navodi da je s obzirom na sve okolnosti ovog incidenta, bio u intenzivnoj komunikaciji sa HAKOM-om te mu je nakon slanja prvog izvještaja o incidentu 09.02.2022. dana uputa u telefonskom razgovoru sa HAKOM-om da se prvo izvješće trebalo slati po proceduri propisanoj Pravilnikom, odnosno šifrirano te da se slijedeća izvješća pošalju

u kriptiranoj formi po proceduri koja je propisana za slanje izvještaja u slučaju sigurnosnog incidenta koji bi značajnije utjecao na rad mreža i/ili usluga, a koja ovdje, po mišljenju A1, s obzirom na okolnosti incidenta nije niti primjenjiva. U odnosu na zatraženo očitovanje o okolnostima sigurnosnog incidenta pod točkom 4. zahtjeva HAKOM-a od 22. veljače 2022., A1 ističe da je žurnim i sveobuhvatnim aktivnostima po saznanju o potencijalnom incidentu, nedvojbeno utvrđeno da je tijekom predmetnog incidenta i povrede podataka ostvaren od strane ovlaštenog korisnika, [redacted]. A1 nadalje naglašava da nije mogla pristupiti nijedna neovlaštena osoba, odnosno [redacted] te da čak i u životno neostvarivom scenariju, odnosno, najmanje vjerojatnom slučaju [redacted], osoba koja neovlašteno pristupa aplikaciji mora istovremeno poznavati [redacted], te dodatno naglašava da je u [redacted] otkrivanje bilo kakvih pristupnih informacija sustavima A1 strogo zabranjeno i podložno oštrom sankcioniranju, kao što i takvu obvezu nameću sami [redacted] prema svojim zaposlenicima. Ključan dokument koji ukazuje na okolnosti i uzroke sigurnosnog incidenta koji ima za posljedicu nastanak povrede podataka jest neovisno forenzičko izvješće [redacted] koje je A1 dostavio u prilogu svog očitovanja, uz naglasak da je A1 samoinicijativno implementirao mjere koje se spominju u analizi, kako slijedi:

- [redacted]

A1 navodi da je sam sigurnosni incident imao kao jedinu posljedicu na korisnike A1 - povredu osobnih podataka dijela korisnika MOZAIK tarife A1, [redacted] Iz prethodno navedenog A1 zaključuje kako je razvidno da niti jedan od gore navedenih podataka ne predstavlja osjetljive podatke korisnika, da nije riječ o podacima čija bi povreda dovela do znatnijih ugroza prava i sloboda pojedinca (kao što bi bilo npr. u slučaju podataka o bankovnom računu, lozinkama i slično) [redacted].

[redacted] dok je istovremeno vršio kontinuiranu komunikaciju sa svim medijima u RH kojima je neovlaštena osoba i počinitelj kaznenog dijela [redacted] uz upozorenje da bi svakom vrstom pristupa i obrade osobnih podataka korisnika MOZAIK tarife A1 unutar javno objavljene datoteke [redacted] prekršili mjerodavne propise. Na taj je način prema navodima A1, osigurano da u navedenom razdoblju ni od jedne strane nije došlo do preuzimanja ili druge vrste obrade osobnih podataka potencijalno izloženih korisnika MOZAIK tarife A1, [redacted] 11.02.2022. uklonjene mogućnosti zlouporabe osobnih podataka korisnika MOZAIK tarife A1, čime A1 zaključuje da su korisnicima MOZAIK tarife A1 bez odgađanja otklonjeni mogući uzroci nastanka štete uslijed opisanog događaja te korisnicima ne prijete niti potencijalni rizici u budućnosti. Između ostalog, osim uspješno izvršenog uklanjanja osobnih podataka potencijalno izloženih korisnika MOZAIK tarife A1 [redacted]. izvršena i detaljna analiza pristupnih logova, odnosno, analiza svih aktivnosti počinitelja kaznenog dijela putem [redacted] i vrlo ograničenom skupu osobnih podataka dijela korisnika A1 za proteklo razdoblje, prilikom koje su utvrđene [redacted]. Zaključno, A1 otklanja mogućnost nepažnje kao uzroka incidenta te ukazuje na nezakonit i neovlašteni pristup od strane treće osobe upravo u cilju izazivanja štete kao izvjestan uzrok nastanka incidenta te u takvoj situaciji preostaje primjena primjerenih organizacijskih i tehničkih sigurnosnih mjera i ublažavanje posljedica za korisnike, a što A1 smatra da je u cijelosti izvršio te utvrđuje da je sukladno važećoj Taksonomiji, [redacted]

Nadalje, A1 je dostavio dokument [redacted] u kojem stoji pojašnjenje na osnovu čega je utvrđeno da se u konkretnom slučaju [redacted] uz pojašnjenje da je za prikaz relevantnih logova korišten [redacted]

[redacted]. A1 navodi da ima [redacted] kojom se proaktivno i u stvarnom vremenu nadziru sigurnosni događaji koji predstavljaju prijetnju A1 poslovanju što uključuje [redacted]

Nadalje, sukladno Taksonomiji [redacted]. A1 je u svom očitovanju dostavio i politike sigurnosti vezane uz sigurnosne zahtjeve za osoblje te dokaze o tome da je [redacted] implementaciju informacijske sigurnosti u skladu s utvrđenim politikama i procedurama A1. Povrh prethodno navedenih mjera i dokaza, A1 navodi da je [redacted] Zaključno, A1 ističe kako uzrok povrede podataka nije nepažnja, nemar ili propust u tehničkim i organizacijskim mjerama, s obzirom da su sve propisane i primjerene mjere osiguranja razine sigurnosti koja odgovara postojećoj razini opasnosti za sigurnost mreže i usluga u skladu s člankom 3. Pravilnika u cijelosti poštivane, već je predmetna povreda nastala kao rezultat zlonamjernih aktivnosti trećih osoba u području kibernetičkog kriminala što je predmet istrage Ministarstva unutarnjih poslova koja je u tijeku.

Nadalje, A1 je sukladno obvezi koja proizlazi iz članka 28. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (dalje: Uredba) i obvezi prema A1 Telekom Austria Grupi u smislu redovitog polugodišnjeg izvješćivanja koje se odnosi na ispunjavanje zahtjeva propisanih internim politikama [redacted]

[redacted] u primjeni sve primjerene tehničke i organizacijske mjere, a osobito napominje da podatke obrađuju samo oni zaposlenici koji su dokazali poštenje, integritet i diskreciju („ovlašteni korisnici“) te isključivo takvi zaposlenici imaju pristup prostorima gdje se nalaze informacijski sustavi ili mediji s osobnim podacima te su svi zaposlenici potpisnici Izjave o povjerljivosti te je provedeno njihovo osposobljavanje kroz koji su isti upoznati sa sigurnosnim uvjetima, svim odgovarajućim politikama i primjenjivim zakonima u vezi s obavljanjem njihovih funkcija i dužnosti u odnosu na obradu osobnih podataka, kao i s posljedicama svakog kršenja ovih uvjeta. Također, navodi da su ovlašteni korisnici posebno informirani o obvezi da elektronička oprema ne smije biti ostavljena bez nadzora i dostupna za vrijeme postupka obrade, a fizički pristup prostorima gdje su pohranjeni osobni podaci ograničen je isključivo na ovlaštene korisnike. [redacted]

Dana 11. ožujka 2022. godine, sukladno članku 6. stavak 4. točka 5. ZEK-a, te čl. 7. Pravilnika inspektor je dostavio Nacionalnom CERT-u (dalje: CERT) predmetnu dokumentaciju i podatke A1 radi stručne analize predmetnih logova s njihove strane te primjenjenih sigurnosnih mjera od strane A1, odnosno eventualnih propusta u primjeni mjera.

CERT se očitovao dana 29. ožujka 2022. godine na način da je uočio određene nedosljednosti u očitovanju A1, poput toga da su utvrđene neuobičajene aktivnosti [redacted].

Dana 7. travnja 2022., inspektor je obavio inspekcijski pregled u prostorijama sjedišta A1 u Zagrebu, Vrtni put 1 gdje je zatražio dodatna očitovanja u odnosu na konkretne okolnosti.

Tako je zatraženo očitovanje u odnosu na način kompromitacije [redacted].

Prisutna osoba tijekom nadzora se u ime [redacted].

[redacted]

Inspektor je zatražio očitovanje i dokumentaciju u prilog tvrdnji A1 da nije došlo do preuzimanja datoteka odnosno da napadač nema podatke na drugom serveru. [redacted]

Dana 13. travnja 2022. godine A1 se očitovao sukladno Zapisniku o objavljenom inspekcijskom nadzoru. Naveo je da se sukladno nalazima [redacted], ne može se zaključiti na koji način je probijena [redacted] te da je s obzirom da nije jasno utvrđen način na koji je došlo do uspješne autentifikacije počinitelja putem sustava za [redacted]

Nadalje, Al navodi da je odmah po utvrđivanju okolnosti sigurnosnog incidenta implementirao [redacted]

[redacted]

Nadalje, u odnosu [redacted]

Analizom zaprimljenih očitovanja kao i inspekcijskim pregledom u prostorijama sjedišta A1 u Zagrebu, inspektor elektroničkih komunikacija (dalje: inspektor) je utvrdio da A1 nije postupio u skladu s člankom 3. i 6. Pravilnika iz sljedećih razloga.

(i) Povreda članka 6. Pravilnika, u vezi s člankom 99. stavak 7. ZEK-a

Člankom 3. Pravilnika propisana je obveza operatora da poduzima odgovarajuće tehničke i ustrojstvene mjere, uključujući šifriranje kada je primjereno, radi zaštite sigurnosti i cjelovitosti svojih mreža i usluga te sprječavanja i umanjenja utjecaja sigurnosnih incidenata na korisnike usluga i međupovezane elektroničke komunikacijske mreže i usluge, pri čemu poduzete mjere moraju osigurati razinu sigurnosti koja odgovara postojećoj razini opasnosti za sigurnost mreže i usluga, dok je člankom 6. Pravilnika propisana obveza operatora da obavijest o sigurnosnim incidentima dostavi Agenciji bez odgode, čim su podaci dostupni u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, u roku od najviše 1 sat nakon otklanjanja sigurnosnog incidenta te u roku od najviše 20 dana od dana otklanjanja sigurnosnog incidenta, upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku elektroničkim putem na adresu elektroničke pošte incidenti@hakom.hr ili na drugi prikladan način.

Kako je utvrđeno u predmetnom postupku, [redacted] u svrhu izrade forenzičkog izvješća, iz čega proizlazi da je A1 bio potpuno svjestan i imao saznanja o nastalom sigurnosnom incidentu najkasnije u trenutku [redacted].

HAKOM je službenu prijavu incidenta od A1 zaprimio tek 9.02.2022. kada je incident već bio objavljen i u medijima, te nakon što je A1 bio upozoren da prijava incidenta nije izvršena na način propisan člankom 6. Pravilnika..

U odnosu na očitovanje A1 o okolnostima pravovremene prijave incidenta, HAKOM smatra da je pogrešno i neosnovano shvaćanje A1 da nije imao obvezu izvijestiti HAKOM o navedenom incidentu budući da sam incident nije zadovoljio ni Kvalitativne ni Kvantitativne kriterije za izvješćivanje iz Dodatka 2 Pravilnika jer nije utjecao na rad A1 mreže ili pružanje usluga. Naime, članak 6. stavak 1. Pravilnika propisuje obvezu pružateljima obavještavanja Agencije o sigurnosnom incidentu koji je značajnije utjecao na rad mreža i/ili usluga sukladno kriterijima za izvješćivanje iz Dodatka 2. Pravilnika, pri čemu pružatelji provjeravaju ispunjavanje Kvantitativnih kriterija te ukoliko isti nisu zadovoljeni provjeravaju ispunjenost Kvalitativnih kriterija iz navedenog Dodatka. U slučaju svakog sigurnosnog incidenta, pružatelji uvijek moraju provjeriti je li došlo do značajnog računalno-sigurnosnog incidenta sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata iz navedenog Dodatka. U tom smislu je potpuno neosnovana tvrdnja A1 da se u konkretnom slučaju nije radilo o sigurnosnom incidentu, budući da iz članka 6. stavka 1. Pravilnika jasno proizlazi da su ispunjeni Kvantitativni kriteriji za izvješćivanje iz Dodatka 2. Pravilnika te da je A1 također morao provjeriti je li došlo i do računalno-sigurnosnog incidenta.

Budući da se u konkretnom slučaju radilo o sigurnosnom incidentu koji utječe na autentičnost i povjerljivost te je incidentom obuhvaćeno više od 1% korisnika (od ukupnog broja korisnika koji koriste te usluge u Hrvatskoj), HAKOM smatra da su zadovoljeni Kvantitativni kriteriji za izvješćivanje te da je A1 temeljem prethodno navedenog imao obvezu izvijestiti HAKOM u propisanom roku.

Također, budući da je sukladno Taksonomiji došlo do značajnog računalno-sigurnosnog incidenta odnosno kompromitacije korisničkog računa i iznude, A1 je trebao prijaviti incident i putem PiXi platforme na način propisan člankom 7. Pravilnika, a što je A1 učinio tek 9.02.2022., i to temeljem naknadne upute HAKOM-a.

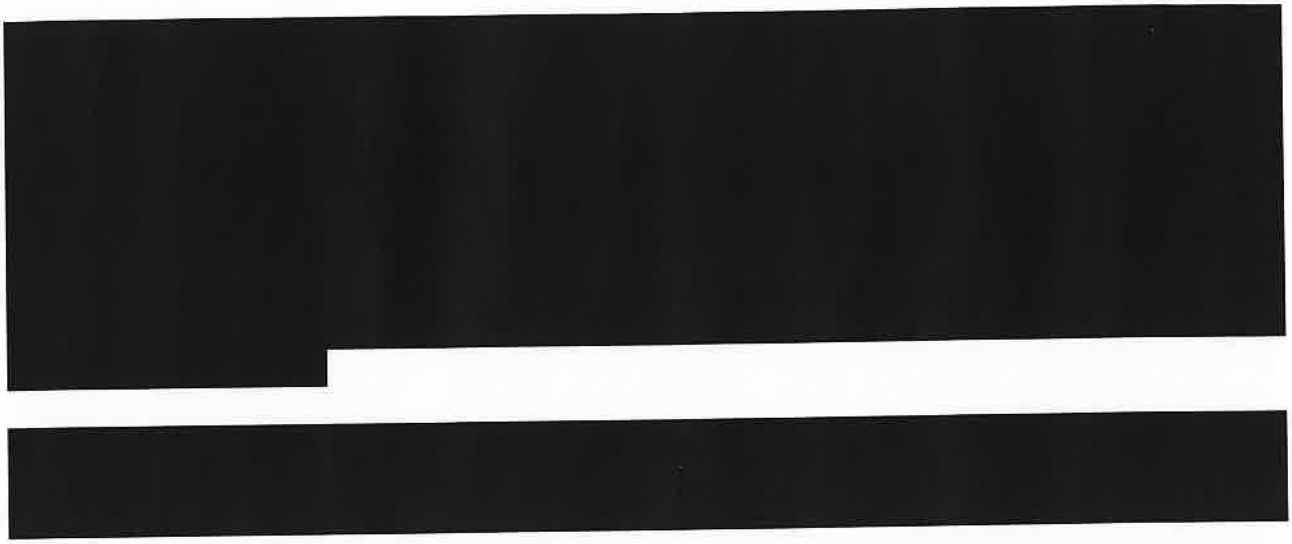
Iz navedenog slijedi da A1 nije postupio sukladno gore citiranoj odredbi članka 6. Pravilnika te nije prijavio predmetni sigurnosni incident u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje propisanih člankom 6. Pravilnika.

(ii) u odnosu na povredu članka 3. Pravilnika, u vezi s člankom 99. stavak 1. ZEK-a

Pored propusta u prijavi sigurnosnog incidenta opisanog ad (i) ovog obrazloženja, inspektor je u predmetnom postupku utvrdio i niz propusta u primjeni odgovarajućih tehničkih i ustrojstvenih mjera, radi zaštite sigurnosti i cjelovitosti mreža i usluga te sprječavanja i umanjenja utjecaja sigurnosnih incidenata na korisnike usluga, kako je propisano člankom 99. stavak 1. ZEK-a te člankom 3. Pravilnika.

[redacted]

[redacted]



Iz svega navedenog slijedi kako je A1 učinio niz propusta u primjeni odgovarajućih sigurnosnih mjera koje bi, da su bile primijenjene, spriječile nastanak sigurnosnog incidenta ili barem njegovo pravovremeno detektiranje te sprečavanje neželjenih posljedica za korisnike usluga.

Nastavno na prethodno navedeni zaključak, inspektor je ovim Rješenjem A1 naložio da se bez odgode uskladi s odredbama članka 3. i 6. Pravilnika, odnosno da poduzima odgovarajuće tehničke i ustrojstvene mjere, radi zaštite sigurnosti i cjelovitosti svojih mreža i usluga te sprječavanja i umanjenja utjecaja sigurnosnih incidenata na korisnike usluga kao i da poduzme odgovarajuće mjere u svrhu osiguranja sigurnosti svojih elektroničkih mreža i usluga na način da primjenjuje procedure kojima će osigurati detektiranje i pravovremeno prijavljivanje sigurnosnih incidenata sukladno ZEK-u i Pravilniku, odnosno da obavijesti o sigurnosnim incidentima dostavlja Agenciji bez odgode, čim su podaci dostupni u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, u roku od najviše 1 sat nakon otklanjanja sigurnosnog incidenta te u roku od najviše 20 dana od dana otklanjanja sigurnosnog incidenta, upotrebom protokola za siguran prijenos podataka ili u šifriranom obliku elektroničkim putem na adresu elektroničke pošte incidenti@hakom.hr ili na drugi prikladan način.

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 75.000 kn (slovima: sedamdesetpet tisuća kuna), a za slučaj daljnjeg neispunjavanja obveze, izricanjem druge, veće novčane kazne.

U odnosu na provjeru postupanja A1 temeljem članka 99.a ZEK-a inspektor elektroničkih komunikacija nije našao da je došlo do povrede postupanja u skladu sa spomenutim člankom, budući da je A1 obavijestio HAKOM o nastaloj povredi te sukladno uputi HAKOM-a o nastalom incidentu obavijestio i krajnje korisnike.

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. A1 Hrvatska d.o.o., Vrtni put 1, 10000 Zagreb, UP-osobnom dostavom
2. U spis