KLASA: UP/I-344-07/20-01/39
URBROJ: 376-05-4-20-3
Zagreb, 23. prosinca 2020.

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; dalje: ZEK), te članka 96. Zakona o općem upravnom postupku (NN br. 47/09), u inspekcijskom postupku, pokrenutom po službenoj dužnosti protiv operatora Telemach Hrvatska d.o.o., Josipa Marohnića 1, 10000 Zagreb, radi provjere postupanja operatora po članku 99. ZEK-a, inspektor elektroničkih komunikacija Hrvatske regulatorne agencije za mrežne djelatnosti (dalje: HAKOM) donosi

RJEŠENJE

I. Utvrđuje se da trgovačko društvo Telemach Hrvatska d.o.o., Josipa Marohnića 1, 10000 Zagreb, nije poštivalo odredbe članka 99. Zakona o elektroničkim komunikacijama (NN br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17; dalje: ZEK) te da nije poduzelo odgovarajuće mjere radi zaštite sigurnosti elektroničkih komunikacijskih mreža i usluga koje bi osigurale pravovremeno detektiranje i prijavljivanje sigurnosnih incidenata.

II. Utvrđuje se da trgovačko društvo Telemach Hrvatska d.o.o., Josipa Marohnića 1, 10000 Zagreb, nije poštivalo rokove za prijavu pojedinog računalno–sigurnosnog incidenta sukladno Pravilniku o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 109/12, 33/13, 126/13, 67/16 i 66/19) (dalje: Pravilnik).

III. Nalaže se trgovačkom društvu Telemach Hrvatska d.o.o., Josipa Marohnića 1, 10000 Zagreb, da odmah po primitku ovog rješenja 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.

Obrazloženje

HAKOM je dana 31. kolovoza 2020. godine pokrenuo inspekcijski nadzor po službenoj dužnosti, a nastavno na obavijest trgovačkog društva Tele2 d.o.o., Josipa Marohnića 1, 10000 Zagreb, zaprimljenu dana 2. srpnja 2020. godine o potencijalnoj povredi osobnih podataka. Društvo Tele2 d.o.o. je tijekom trajanja predmetnog postupka, dana 2. studenog 2020. promijenilo tvrtku društva u Telemach Hrvatska d.o.o. (dalje: Telemach).

Telemach je u prethodno spomenutoj obavijesti naveo da je prilikom analize i rješavanja sigurnosnog incidenta uzrokovanog iskorištavanjem ranjivosti softvera treće strane koji je korišten u razvoju aplikacije web shopa, dana 1. srpnja 2020. utvrdio da su na kompromitiranom sustavu smješteni i određeni dokumenti koji sadržavaju i osobne podatke nekih korisnika Telemach-a te da je po otkrivanju sigurnosnog incidenta, pokrenuo procedure za zaštitu poslovanja i korisničkih podataka, detaljne analize utjecaja sigurnosnog incidenta na poslovanje, preuzeo sve povijesne datoteke i angažirao specijaliziranu kompaniju za istraživanje utjecaja sigurnosnih incidenata, a po čijoj je izvršenoj inicijalnoj analizi, ustanovljeno da se radi o softverskom propustu na Web aplikaciji Telemach-a što je omogućilo implementaciju softvera od strane nepoznatog počinitelja na operativni sustav. Također, naveo je da su prema nalazima i preporukama, poduzete sljedeće aktivnosti za sprečavanje softverskog napada:

1. Postavljeni su softverski alati kojima se detaljno prati potencijalna aktivacija instaliranog softvera
2. Izvršene su aktivnosti na podizanju korištenog komercijalnog softvera (Windows) na zadnju dostupnu verziju
3. Angažiran je dobavljač sustava Web trgovina radi podizanja sigurnosnih zakrpi na svim dijelovima sustava
4. Izvršena je priprema nove platforme za implementaciju sustava Web trgovina uz postavljanje dodatnih zaštita (promjena IP adresa, izolacija od ostalog dijela podatkovnog centra,…)
5. Radi se na promjeni svih korisničkih imena i zaporki koje sustav Web trgovina koristi za povezivanje sa ostalim sustavima
6. Radi se na implementaciji dodatne zaštite u komunikaciji između sustava kroz upotrebu certifikata.

Napomenuo je i da sve provedene aktivnosti, uz dodatni pojačani nadzor, osiguravaju da se predmetni napad ne može ponoviti te da smatra da je sustav zaštićen svim raspoloživim sredstvima, a nakon što se završe sve aktivnosti i analize na postojećem sustavu, isti će biti uklonjen (trenutno će biti izbačen iz komercijalnog rada, ali će se sačuvati u izoliranom stanju kako bi se mogle izvršiti sve potrebne analize).

Nastavno na obavijest Telemach-a zaprimljenu dana 2. srpnja 2020. godine o potencijalnoj povredi osobnih podataka, HAKOM je dana 3. srpnja 2020. godine zatražio dostavu dodatnih informacija u vezi nastalog incidenta na način propisan Pravilnikom, a što je Telemach učinio istog dana. U navedenom izvještaju od dana 6. srpnja 2020. je uz opis incidenta, kao datum nastanka/otkrivanja sigurnosnog incidenta naveden 26. lipnja 2020. godine dok broj obuhvaćenih korisnika nije naveden, uz pojašnjenje kako je još uvijek u tijeku analiza incidenta. HAKOM je stoga, 8. srpnja 2020. godine zatražio dostavu barem procjene broja korisnika kao i kategoriju osobnih podataka koji su bili obuhvaćeni incidentom.

Dana 24. srpnja 2020. godine, Telemach je dostavio dodatne informacije u kojima je naveo da je nakon provedene forenzike incidenta uočio da su poslužitelji SEWP-HRWSFR01 i SEWP-HRWSFR02 kompromitirani iskorištavanjem CVE-2019-18935 ranjivosti (*Remote Code Execution via Insecure Deserialization in Telerik UI*), za koju je javno dostupan *exploit* koji omogućava iskorištavanje ranjivosti. Direktoriji u kojima su identificirane datoteke s osobnim podacima sadrže ugovore za zasnivanje pretplatničkog odnosa (maksimalno 25.032 korisnika), skenove/fotografije osobnih iskaznica (maksimalno 44.236 korisnika), HTM datoteke s ugovornom dokumentacijom za zasnivanje pretplatničkog odnosa (maksimalno 12.116 datoteka zahtjeva za zasnivanje pretplatničkih odnosa). Nadalje, u svom očitovanju Telemach navodi da je pronađena *web shell* aplikacija s datumom nastanka 1. veljače 2020. godine, međutim zbog nedostatka logova nije moguće

identificirati kako je navedena datoteka postavljena na poslužitelj. Najranije maliciozne aktivnosti identificirane su 29. travnja 2020. kada je napadač na ranjive poslužitelje postavio tzv. *web shell* aplikaciju (shell.aspx na poslužitelju), koja mu je omogućila daljnje izvršavanje komandi pod privilegijama IIS korisnika pod kojim je bila pokrenuta i web aplikacije. Naveo je da Telemach tek 1. srpnja 2020. utvrdio da su na kompromitiranom sustavu smješteni i određeni dokumenti koji sadržavaju i osobne podatke nekih korisnika Telemach te da je 2. srpnja o tome obavijestio HAKOM. Nadalje, naveo je da su incidentom zahvaćeni procesi Telemach web stranica, Telemach web shop, TLS beskontaktno plaćanje, Samostalna dostava robe te da ni u kojem trenutku nije uočeno ugrožavanje, zaustavljanje ili usporavanje navedenih procesa ili usluga. Od propusta koje imao, Telemach je naveo propust u primjeni sljedećih mjera: proaktivan nadzor i praćenje sigurnosnih događaja od strane Tele2 Švedska, poštivanje propisanog Pravilnikom o upravljanju log zapisima i sigurnosnim događajima te Pravilnika o upravljanju ranjivostima.

Nakon analize dostavljenih očitovanja, a imajući u vidu činjenicu da se iz dostavljenih podataka nije moglo nesporno utvrditi da osobni podaci korisnika nisu kompromitirani, odnosno da ne postoji mogućnost da dođe do njihove zlouporabe u budućnosti, HAKOM je 4. kolovoza poslao mišljenje u kojem je zatražio od Telemach-a da u najkraćem mogućem roku obavijesti korisnike o povredi osobnih podataka, sve sukladno članku 99.a stavku 1., 2. i 4. ZEK-a te da povratno obavijesti HAKOM o načinu, sadržaju i trenutku slanja takve obavijesti.

Dopisom od dana 27. kolovoza 2020. godine Telemach je obavijestio HAKOM da će u sklopu dostave računa za mjesec kolovoz 2020.g., a za koje procjenjuju da će od 3. rujna krenuti u distribuciju, identificirane osobe zahvaćene incidentom obavijestiti o povredi njihovih osobnih podataka. Ako identificirana osoba više nije Telemach korisnik ista će na adresu dobiti samo obavijest (bez računa). Smatraju da će na taj način transparentno i detaljno informirati korisnike o nastalom incidentu. Sadržaj obavijesti je, između ostalog, sadržavala informaciju o događaju sigurnosnog incidenta uslijed hakerskog napada na web serverima Telemach-a, činjenici da su u roku incident prijavili nadležnim državnim službama, kategoriji osobnih podataka koji su bili obuhvaćeni incidentom te kontaktne podatke za dodatne obavijesti. Na prethodno spomenuti dopis HAKOM se očitovao mišljenjem da radi transparentnijeg i učinkovitijeg obavještavanja korisnika smatra da je obavijest potrebno poslati kao poseban dopis u okviru pošiljke kojom se šalje račun te da ista ne bude sadržana na samom računu.

Dana 31. kolovoza 2020.godine HAKOM je pokrenuo inspekcijski nadzor nad Telemach-om te zatražio dostavu dokaza vezanih uz trenutak kada je otkriven računalno-sigurnosni incident. Također, nastavno na očitovanje Telemach-a od 27. srpnja 2020. u kojem su naveli koje mjere zaštite su poduzeli nakon otklanjanja sigurnosnog incidenta, HAKOM je zatražio dostavu i dokaza o poduzetom kao i dokaz o broju korisnika čiji osobni podaci su bili obuhvaćeni incidentom. Nadalje, zatraženo je i očitovanje zašto u reviziji informacijskog sustava, koja je rađena 15. svibnja 2020. godine (nakon pojave računalno-sigurnosnog incidenta) nisu primijećeni nedostaci koji su doveli do pojave predmetnog računalno-sigurnosnog incidenta.

Telemach je dana 10. rujna 2020. dostavio očitovanje putem elektroničke pošte te također originale, poštom 11. rujna 2020. godine. U istom je navedeno da je sukladno propisanim odgovornostima dana 26. lipnja 2020. godine švedski tim za incidente (CSIRT) je upozorio Telemach u Hrvatskoj kako je na jednom od servera s kojeg se pruža usluga web shopa nađen „Meterpreter program“ te da se sumnja kako je isti ostao od penetracijskog testiranja koji se provodio na tim serverima. Nadalje, navodi da zbog propusta na operativnoj razini u okviru sustava Tele2 Švedska o gore navedenom prije 26. lipnja

2020. nije imao saznanja, niti subjektivna niti objektivna te da omaškom CSIRT tima, detekcije koje su uočene na antivirusnoj konzoli nisu pravovremeno javljene Telemach-u u Hrvatskoj. Također, navodi da u Pravilniku između ostalog stoji da su operatori obavezno obavijestiti Agenciju u trenutku čim su podaci o incidentu dostupni te da smatra da je trenutak nastupio nakon što je prikupio sve relevantne podatke potrebne za adekvatno ispunjavanje propisane prijave te da prije 3. srpnja 2020. još nije znao je li riječ o sigurnosnom incidentu, jer je prvotna sumnja bila usmjerena na ostatke penetracijskog testa koji je bio proveden u 2019. godini (artefakte preostale od samog testa). U tjednu od 29. lipnja do 3. srpnja specijalizirana kompanija INFIGO je provela forenzičku analizu dostavljenih memorijskih slika i slika tvrdih diskova servera koja je potvrdila je da su serveri bili višestruko kompromitirani te da se najranije maliciozne aktivnosti pojavljuju 29. travnja 2020. godine. Telemach ističe da čim je imao potvrdu da je riječ o incidentu, isti je odmah prijavio (3. srpnja 2020.), sukladno Pravilniku. U dijelu poduzetih mjera zaštite, Telemach navodi da sve provedene aktivnosti, uz dodatan pojačani nadzor, smanjuju vjerojatnost ponavljanja incidenta ili njegovog utjecaja te da smatra da je sustav zaštitio svim razumnim sredstvima slijedom čega može utvrditi da je adekvatnom reakcijom proveo odgovarajuće tehničke i ustrojstvene mjere za osiguranje sigurnosti i integriteta svoje mreže i usluga, a čime je osigurao neprekidno pružanje usluga putem svoje mreže i to ublažavajući utjecaj incidenta na rad mreže, mrežno povezivanje kao i na usluge korisnika. Također, navodi da smatra da su poduzete mjere spriječile i umanjile utjecaj incidenta na korisnike usluga i međusobno povezane elektroničke komunikacijske mreže, pa shodno tome nije došlo do povrede odredbe članaka 99. i 99a ZEK-a. U djelu očitovanja vezan uz korisnike zahvaćene incidentom navodi da je prvotna, odnosno inicijalna procjena broja korisnika čiji su se podaci nalazili na poslužiteljima dana kao maksimalan broj, te da je pritom važno naglasiti da nije izvjesno da je to ujedno i broj korisnika čiji su osobni podaci bili na poslužiteljima jer je moguće da se unutar tog broja nalaze i korisnici pravne osobe. Također, navodi da podaci vezani uz te korisnike nisu ujedno nužno i osobni podaci prema Općoj uredbi o zaštiti podataka jer istom nije obuhvaćena obrada osobnih podataka koji se tiču pravnih osoba te da stoga zaključuje da su ga datoteke koje su bile zahvaćene incidentom i manualno pretražene, a sve kako bi utvrdili točan broj identificiranih korisnika, dovele do konačne brojke identificiranih 28.085 osoba. Nadalje, ističe da je, imajući u vidu odredbu članka 99.a ZEK-a, od presudne važnosti činjenica da nastala povreda osobnih podataka nije štetno utjecala na osobne podatke ili privatnost korisnika usluga ili druge fizičke osobe, čime korisnici nisu pretrpjeli imovinski ili neimovinski gubitak.

Vezano uz provedenu reviziju sigurnosnih politika Telemach je istaknuo da je revizijski angažman ograničen na područje (opseg) i vremenski period obuhvaćen revizijom te da se provjere provode na osnovu uzorka i nasumičnog odabira sustava ili primjera za pregled, temeljem čega revizijski izvještaj rezultira razumnim uvjerenjem o razini rizika u pregledanom području, ali ne daje potpuno uvjerenje da rizici ne postoje ako nisu identificirani za vrijeme revizije. Zaključno je naveo da incident nije predstavljao neposrednu i ozbiljnu prijetnju javnom redu, javnoj sigurnosti ili javnom zdravlju te da incident nije stvorio ozbiljne gospodarske ili operativne probleme drugim pružateljima ili korisnicima elektroničkih komunikacijskih mreža ili usluga ili drugim korisnicima radiofrekvencijskog spektra te da može istaknuti da predmetni incident nije imao posljedicu na djelovanje i raspoloživost usluga koje se pružaju korisnicima, a čime nije narušen kontinuitet pružanja usluge kao niti integritet mreže niti tajnost komunikacija te da su pored toga poduzete su sve razumne mjere kako bi se smanjila vjerojatnost ponavljanja istog.

Nakon analize zaprimljenih dokaza, inspektor elektroničkih komunikacija (dalje: inspektor) je utvrdio da postupanje Telemach-a nije bilo u skladu s ZEK-om i Pravilnikom iz sljedećih razloga.

Odredbom članaka 99. stavka 1. ZEK-a propisano je da su operatori obvezni provesti odgovarajuće tehničke i ustrojstvene mjere za osiguranje sigurnosti i integriteta svojih javnih komunikacijskih mreža i/ili usluga. Te mjere moraju osigurati neprekidno pružanje javnih komunikacijskih usluga putem mreža, kao i stupanj sigurnosti, odgovarajući na prijetnje i sprječavajući sigurnosne incidente ili ublažavajući njihov utjecaj na rad javne komunikacijske mreže, mrežno povezivanje kao i/ili na javne komunikacijske usluge korisnika. Inspektor smatra da Telemach nije osigurao sigurnost svoje mreže i usluga budući da je iz dokaza dostavljenih 10. rujna 2020. razvidno da u periodu od 01. veljače 2020. godine od kada datira pronađena *web shell* aplikacija, kao i tijekom 29. travnja 2020. kada su naknadnom forenzikom identificirane najranije maliciozne aktivnosti pa do 26. lipnja 2020. godine nije imao saznanja o istome, odnosno nije imao proaktivan nadzor i praćenje sigurnosnih događaja, nije poštivao propisano Pravilnikom o upravljanju log zapisima i sigurnosnim događajima te Pravilnikom o upravljanju ranjivostima, a što je i sam naveo u svojim izvješćima i dostavljenim očitovanjima.

Nadalje, odredbom članka 5. stavka 2. Pravilnika propisano je da o računalno-sigurnosnim incidentima operatori moraju obavijestiti Agenciju bez odgode, čim su podaci dostupni, i to putem obrasca propisanog u Dodatku 3. Pravilnika i to u roku od najviše 24 sata nakon otkrivanja računalno-sigurnosnog incidenta kao i u roku od najviše 20 dana od dana otklanjanja računalno-sigurnosnog incidenta. Inspektor smatra da Telemach nije u roku obavijestio HAKOM o računalno-sigurnosnom incidentu budući da je iz dokaza dostavljenih 10. rujna 2020. razvidno da je Telemach u Hrvatskoj putem elektroničke pošte 26. lipnja 2020. zaprimio obavijest o malicioznim aktivnostima od Rickarda Zetterlunda, *IT Security Specialist-a* u Tele2 Švedska, a za koje je sukladno kriterijima za izvješćivanje iz Dodatka 2. Pravilnika kao uvjet prijave računalno-sigurnosnog incidenta propisano - *zlonamjerna funkcionalnost aktivna je duže od 12 sati*. Također, Telemach je obavijest o potencijalnoj povredi osobnih podataka dostavio HAKOM-u dana 2. srpnja 2020. godine te tek nakon što je 3. srpnja 2020. godine HAKOM zatražio dostavu dodatnih informacija u vezi nastalog incidenta na način propisan Pravilnikom, Telemach je na propisan način prijavio računalno-sigurnosni incident isti dan.

Navodi Telemach-a iz dostavljenog očitovanja da prijava propisana Pravilnikom nije podnesena prije 3. srpnja 2020. zbog činjenice da su u tijeku bile dodatne analize kao i prikupljanje podataka, nisu relevantni za procjenu povrede članka 99. ZEK-a i Pravilnika, budući da su kriteriji propisani Pravilnikom jasni i precizni te se odnose isključivo na duljinu trajanja određenog računalno-sigurnosnog incidenta, a za koji je Telemach imao saznanja već dana 26. lipnja 2020.

Nastavno na prethodno navedeno, inspektor je rješenjem utvrdio povrede članka 99. ZEK-a te članka 5. Pravilnika budući da Telemach nije poduzeo odgovarajuće mjere radi zaštite sigurnosti elektroničkih komunikacijskih mreža i usluga koje bi osigurale pravovremeno detektiranje sigurnosnih incidenata, kao i njihovo pravovremeno prijavljivanje HAKOM-u. Slijedom navedenog, točkom III. izreke naloženo je Telemach-u poduzimanje mjera 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.

Na temelju 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. Telemach Hrvatska d.o.o., Josipa Marohnića 1, 10000 Zagreb, UP-osobnom dostavom
2. U spis