Upute za važne subjekte sektora elektroničkih komunikacija

SADRŽAJ

UVOD

Svrha ovih uputa je na jednom mjestu upoznati pružatelje javnih elektroničkih komunikacijskih usluga i mreža (dalje u tekstu: operatori) sa zahtjevima i praktičnim postupkom provedbe istih prema Zakonu o kibernetičkoj sigurnosti (Narodne novine, br. 14/2024, dalje u tekstu: ZKS) i Uredbi o kibernetičkoj sigurnosti (Narodne novine, br. 135/24, dalje u tekstu: Uredba) koje možete naći na linku: ZKS i Uredba

U odnosu na druge sektore obuhvaćene ZKS-om, sektor elektroničkih komunikacija (dalje: ECS/N sektor) ima specifičnost na način da su svi subjekti ECS/N sektora obuhvaćeni ZKS-om bez obzira na veličinu, odnosno svi subjekti postaju ključni ili važni subjekti, neovisno o državi poslovnog nastana.

Na temelju članaka 17. do 24. Uredbe u svrhu provedbe obveza iz članka 20. ZKS-a obveznici dostave podataka, odnosno subjekti kategorizirani temeljem ZKS-a i Uredbe, dužni su dostavljati podatke HAKOM-u, kao nadležnom tijelu za provedbu kategorizacije.

IMENOVANJE KONTAKT OSOBE ODGOVORNE ZA DOSTAVU PODATAKA

Subjekti kategorizirani temeljem ZKS-a i Uredbe dužni su imenovati kontakt osobu odgovornu za dostavu podataka i obavijesti o promjenama podataka. Imenovana kontakt osoba mora biti iz reda članova upravljačkog tijela subjekta te je dužna imenovati najmanje dvije osobe ovlaštene za operacionalizaciju dostave podataka i obavijesti o promjenama podataka.

SADRŽAJ DOSTAVE PODATAKA

Subjekti kategorizirani temeljem Zakona i Uredbe dužni su nakon zaprimanja obavijesti kroz sustav e-Operator (možete naći na linku: Upute za e-Operator) dostaviti slijedeće podatke:

- podatke o imenovanoj kontakt osobi odgovornoj za dostavu podataka i osobama ovlaštenim za operacionalizaciju dostave podataka i obavijesti o promjenama podataka:
- ime i prezime imenovanih osoba
- podatke o njihovom radnom mjestu, odnosno dužnosti u subjektu
- broj telefona, broj mobitela i adresa elektroničke pošte imenovane kontakt osobi odgovorne za dostavu podataka
- broj telefona, broj mobitela i adrese elektroničke pošte koje će osobe ovlaštene za operacionalizaciju dostave koristiti u svrhe dostave podataka i obavijesti o promjenama podataka.
- podatke o subjektu:
  1) naziv subjekta
  2) OIB subjekta
  3) podatci o veličini subjekta
  4) adresa subjekta
  5) broj telefona, broj mobitela i adresa elektroničke pošte imenovane kontakt osobi odgovorne za dostavu podataka
  6) IP adresni rasponi koje subjekt koristi u Republici Hrvatskoj
  7) relevantni sektor, podsektor i vrstu subjekta iz Priloga I. i Priloga II. Zakona
  8) popis država članica u kojima subjekt pruža usluge odnosno obavlja djelatnosti iz Priloga I. odnosno Priloga II. Zakona
  9) pravne osobe koje subjektu pružaju ili će pružati upravljane i upravljane sigurnosne usluge iz Priloga I. Zakona, sektor broj 9., Upravljanje IKT uslugama, izuzev usluga informacijskih posrednika
  10) drugi podatci o pružanju svojih usluga ili obavljanju svojih djelatnosti (podatci o veličini subjekta i djelatnosti za koju je subjekt kategoriziran).

NAČIN I ROKOVI DOSTAVE PODATAKA

Subjekti kategorizirani temeljem ZKS-a dužni su potrebne podatke dostavljati HAKOM-u putem sustava e-Operator kojim se pristupa prijavom putem vlastitog korisničkog računa putem poveznice: https://eoperator.hakom.hr/eop/eopinfo

Navedeni podaci se dostavljaju jednom godišnje za prethodnu godinu, a najkasnije do 31.03. tekuće godine. Novi operatori prve podatke dostavljaju nakon registracije u sustav e-Operator te nakon toga nastavljaju na godišnjoj razini.

U slučaju promjene imenovanih osoba ili dostavljenih podataka operatori su dužni predmetnu izmjenu unijeti kroz sustav e-Operator, bez odgode, a najkasnije u roku od 15 dana od imenovanja nove osobe, odnosno promjene pojedinih podataka.

OBVEZE IMPLEMENTACIJE SIGURNOSNIH MJERA i SAMOPROCJENA

1. Razine mjera upravljanja kibernetičkim rizicima

Po provedenom postupku kategorizacije HAKOM utvrđuje da li određeni operator predstavlja ključni ili važni subjekt sukladno ZKS-u, za sektor digitalne infrastrukture, vrstu subjekta: pružatelj javnih elektroničkih komunikacijskih mreža i/ili usluga. U okviru postupka kategorizacije operatora HAKOM provodi nacionalnu procjenu kibernetičkih sigurnosnih rizika za svakog operatora. Cilj provođenja nacionalne procjene rizika je definirati razinu mjera upravljanja kibernetičkim sigurnosnim rizicima koju je dužan provoditi operator koji je kategoriziran kao ključni, odnosno važni subjekt. Sukladno kategorizaciji, dodjeljuje se razina kibernetičke sigurnosti koju moraju postići: **osnovna, srednja ili napredna.**

Osnovna razina mjera primjenjuje se na subjekte s nižim profilom rizika te se temelji na lako dostupnim tehnologijama i dobro poznatim sigurnosnim praksama. Cilj je zaštita od najčešćih globalnih napada koje provode napadači s prosječnim vještinama.

Srednja razina mjera nadograđuje osnovnu razinu dodatnim mjerama radi povećane otpornosti. Namijenjena je subjektima iz sektora gdje postoji veći rizik od ciljanih napada prosječno vještih napadača. Napredna razina mjera je najviša razina zaštite, uključuje napredne tehničke i organizacijske mjere. Cilj je obrana od sofisticiranih i resursno jakih napadača s visokim razinama vještina.

S obzirom na utvrđenu razinu kibernetičkih sigurnosnih rizika operatori su dužni provesti osnovnu, srednju ili naprednu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. stavka 1. i Priloga II. Uredbe. **Dodijeljenu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima operatori su dužni provesti u roku godine dana od dana kategorizacije.**

Potrebno je posebno napomenuti kako operator može biti kategorizirani u više sektora, podsektora i vrsta subjekata te sukladno tome može dobiti više obavijesti o kategorizaciji. U tom slučaju primijenit će se članak 59. stavak 3. ZKS-a te će se putem protokola **odrediti jedno nadležno tijelo (glavno nadležno tijelo)** koje će o istom obavijestiti višekategoriziranog operatora. Izrada protokola ne odgađa rokove i obveze kategoriziranog operatora, a razina mjera kibernetičke sigurnosti primjenjuje se sukladno članku 39. stavku 2. Uredbe, odnosno provodi se **najviša razina mjera utvrđena između višestrukih kategorizacija koje operator zaprimi.** Također, ukoliko je pojedini operator barem jednoj od višestrukih kategorizacija koje je zaprimio određen kao ključni subjekt, **odgovoran je provoditi zakonske obveze za ključne subjekte.**

2. Samoprocjena

Sukladno članku 35. ZKS-a, kao važan subjekt operator je obvezan provoditi samoprocjenu kibernetičke sigurnosti **najmanje jednom u dvije godine**. Navedena obveza počinje s danom primitka obavijesti o provedenoj kategorizaciji subjekata putem sustava e-Operator i/ili pisanim putem. Za provedbu samoprocjene kibernetičke sigurnosti operator je obvezan odrediti svoje zaposlenike ili vanjske suradnike sukladno članku 56. Uredbe te samoprocjenu provesti sukladno odredbama Uredbe. Drugim riječima, za provedbu samoprocjene kibernetičke sigurnosti subjekt je dužan odrediti svoje zaposlenike ili vanjske suradnike koji posjeduju najmanje:

– relevantna znanja iz implementacije međunarodnih normi iz područja informacijske ili kibernetičke sigurnosti

– potvrdu o završenoj vanjskoj ili internoj edukaciji za internog revizora po nekoj od relevantnih međunarodnih normi iz područja informacijske ili kibernetičke sigurnosti

– jednu godinu radnog iskustva u okviru provođenja sličnih vrsta interne revizije u području mrežnih i informacijskih sustava odnosno kibernetičke sigurnosti.

Također, sukladno članku 34. stavak 4. Zakona, operatori koji su kategorizirani kao važni subjekt dužni su provesti vanjsku reviziju kibernetičke sigurnosti, ukoliko to HAKOM kao nadležno tijelo od njih zatraži..

Samoprocjenu kibernetičke sigurnosti mogu provoditi i operatori kategorizirani kao ključni subjekt kao pripremu za provedbu vanjske revizije kibernetičke sigurnosti.

Stupanj usklađenosti uspostavljenih mjera iz članka 52. stavaka 2. i 3. Uredbe utvrđuje se temeljem bodovanja podskupova mjera upravljanja kibernetičkim sigurnosnim rizicima koje subjekt provodi kao obvezujuće sukladno članku 44. stavcima 1. i 2. Uredbe, sukladno Smjernicama za samoprocjenu kibernetičke sigurnosti Zavoda za sigurnost informacijskih sustava koje možete naći na linku: Smjernice za samoprocjenu

Svaka razina mjere (osnovna, srednja i napredna) ima propisanu minimalnu ocjenu koju subjekt mora zadovoljiti kako bi se mogla uzimati u prosjek. Sustav ocjenjivanja podmjera temelji se na ispunjavanju uvjeta pojedinačnih kontrola i ukupne ocjene podmjere za odgovarajuću razinu.

Pomoću Kalkulatora za samoprocjenu koji je dio Smjernica za samoprocjenu izračunava se konačni rezultat samoprocjene, odnosno ukupni bodovi stupnja usklađenosti mjera. Ispunjeni Kalkulator za samoprocjenu pohranjuje se na infrastrukturi koja je pod kontrolom subjekta koji vrši samoprocjenu. Pristup osjetljivim podacima iz Kalkulatora za samoprocjenu trebao bi biti dopušten samo ovlaštenim osobama

Trend podizanja razine zrelosti kibernetičke sigurnosti utvrđuje se dodatnim bodovanjem podskupova mjera upravljanja kibernetičkim sigurnosnim rizicima koje subjekt provodi na temelju mjere 3. »Upravljanje rizicima« iz Priloga II. Uredbe, u smislu podizanja razine provedbe pojedinih obvezujućih mjera sukladno članku 44. stavcima

1. i 2. Uredbe, kao i u smislu provedbe dobrovoljnih mjera sukladno članku 44. stavku 3. ove Uredbe. U svrhu provedbe bodovanja trenda podizanja razine zrelosti, za svaku razinu mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. Uredbe utvrđuje se broj bodova potreban za utvrđivanje trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta.
Ako rezultati bodovanja stupnja usklađenosti mjera sukladno članku 53. Uredbe pokazuju da su uspostavljene mjere upravljanja kibernetičkim sigurnosnim rizicima u skladu s razinom mjera upravljanja kibernetičkim sigurnosnim rizicima koja je utvrđena obvezujućom za operatora**, operator sastavlja izjavu o sukladnosti** iz članka 35. stavka 3. ZKS-a na obrascu iz Priloga IV Uredbe te potpisanu dostavlja putem sustava e-Operator. Ako rezultati bodovanja stupnja usklađenosti mjera pokazuju da nisu uspostavljene mjere na zadovoljavajući način, operator utvrđuje plan daljnjeg postupanja, koji uključuje plan za pravodobnu ponovnu samoprocjenu kibernetičke sigurnosti i ispravljanje utvrđenih nedostataka. Izjavu o sukladnosti i drugu dokumentaciju nastalu u postupku samoprocjene kibernetičke sigurnosti operator je dužan čuvati deset godina od sastavljanja iste.

KAKO IZGLEDA DOBAR REZULTAT?
Sve obvezne mjere su dokumentirane i provedene što podrazumijeva da svaka pojedina mjera unutar Kalkulatora za samoprocjenu mora biti pozitivno ocijenjena (označena zelenom bojom). Pripremljena je potrebna dokumentacija, pokazan je trend zrelosti (dodatne/dobrovoljne mjere) te u organizaciji postoji razumijevanje odgovornosti.
KAKO POSTIĆI USKLAĐENOST?
Nakon dobivene obavijesti o kategorizacije osobito je potrebno :

- detaljno pročitati sadržaj zaprimljene obavijesti
- napraviti GAP analizu
- početi prikupljati dokumentaciju za mjere iz Priloga II.
- provesti obvezne mjere
- pratiti objavu službenih smjernica i kalkulatora od strane nadležnih tijela (NCSC-HR,ZSIS, HAKOM)
-

Za sva dodatna pitanja potrebno je kontaktirati putem adrese elektroničke pošte HAKOM-NIS2@hakom.hr.

OBAVJEŠTAVANJE O ZNAČAJNIM INCIDENTIMA I PRIJETNJAMA

Sukladno članku 37. ZKS, operatori su **dužni u roku 30 dana od dana kategorizacije** započeti s obavještavanjem o značajnim incidentima, sukladno „Općim smjernicama za provedbu obveze obavještavanja o značajnim incidentima“ objavljenim na mrežnoj stranici Nacionalnog centra za kibernetičku sigurnost (https://ncsc.hr), pod kategorijom Dokumenti, Smjernice. Za ECS/N sektor nadležan je CSIRT pri središnjem državnom tijelu za kibernetičku sigurnost (Nacionalni centar za kibernetičku sigurnost, NCSC).

Kategorizirani operatori su stekli status subjekta korisnika nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima (dalje u tekstu: PiXi), slijedom čega proizlaze obveze iz članaka 96. i 97. Uredbe. Za pristup PiXi platformi koristi se autentifikacijski i autorizacijski proces Nacionalnog identifikacijskog i autentifikacijskog sustava (NIAS). Preduvjet za korištenje PiXi platforme je da pravna osoba ima uspostavljeno e-Poslovanje koje omogućava autentifikaciju poslovnim vjerodajnicama, odnosno autentifikaciju korisnika u svojstvu poslovnog subjekta. Kroz sustav e-Poslovanje (uputa „Protokol rada NIAS-a za e-Građane i e-Poslovanje“ raspoloživa preko tražilice) ulazi se u komponentu e-Ovlaštenja (uputa „Protokol rada e-Ovlaštenja“ raspoloživa preko tražilice), koja služi za autorizaciju autentificiranog korisnika za uslugu „Platforma PiXi“, koju treba odabrati, a pri tome se moraju koristiti vjerodajnice visoke ili značajne razine sigurnosti.
Operatori se za pomoć u vezi pristupa sustavu NIAS mogu obratiti na adrese elektroničke pošte pomoc@e-gradjani.gov.hr, pomoc@e-poslovanje.gov.hr ili telefonom: 072 200 027 radnim danom od 8:00 do 20:00 te subotom od 8:00 do 13:00. Za pomoć u vezi korištenja PiXi platforme možete se obratiti na adresu elektroničke pošte helpdesk@carnet.hr ili telefonom: 01 6661 555 svih sedam dana u tjednu od 8:00 do 22:00.

Prekršajne odredbe

Prekršajnim odredbama ZKS-a predviđene su novčane kazne za ključne i važne subjekte koji ne postupaju u skladu sa propisanim zahtjevima kibernetičke sigurnosti, a u određenim slučajevima, značajni incidenti ili ozbiljnije kibernetičke prijetnje mogu se kategorizirati kao kaznena djela protiv računalnih sustava, programa i podataka (Glava XXV Kaznenog zakona NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18,126/19, 84/21, 114/22, 114/23, 36/24, 136/25).Na naknadu štete primjenjuju se opća pravila o naknadi štete sukladno posebnim propisima.