NIS2

- tržište elektroničkih komunikacija-

Zagreb, Hrvatska

17. listopada 2024.

HAKOM

NIS2

NIS2 Direktiva

Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148- NIS1

- Rok za usklađivanje s NIS2 Direktivom je 17. listopada 2024.

ZKS

Zakon o kibernetičkoj sigurnosti (NN br. 14/24)

- stupio na snagu 15. veljače 2024.
- danom stupanja na snagu prestaje važiti članak 41. Zakona o elektroničkim komunikacijama
- Uredba o kibernetičkoj sigurnosti – trenutno u postupku javnog savjetovanja

Odnos ZEK - ZKS

- HAKOM je temeljem čl. 41. Zakona o elektroničkim komunikacijama (NN br. 76/22) regulirao sigurnost elektroničkih komunikacijskih mreža i usluga
- temeljem predmetnog članka ZEK-a, HAKOM je donio Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti mreža i usluga (NN br. 52/23) - implementacija 5G toolbox-a
- Prijelazna odredba ZKS-a:

"Pružatelji javnih elektroničkih komunikacijskih mreža i pružatelji javno dostupnih elektroničkih komunikacijskih usluga koji su do stupanja na snagu ovog Zakona provodili sigurnosne zahtjeve u svrhu zaštite sigurnosti elektroničkih komunikacijskih mreža i elektroničkih komunikacijskih usluga prema odredbama članka 41. Zakona o elektroničkim komunikacijama („Narodne novine", broj: 76/2022) nastavljaju s provedbom zahtjeva na temelju članka 41. tog Zakona do dostave obavijesti o provedenoj kategorizaciji subjekta iz članka 19. stavka 1. ovog Zakona." - članak 106. stavak 1. ZKS-a

KLJUČNI I VAŽNI SUBJEKTI

- svi operatori na tržištu elektroničkih komunikacija obuhvaćeni su obvezama ZKS-a

- **KLJUČNI SUBJEKTI** - operatori koji su srednji i veliki subjekt malog gospodarstva (broj zaposlenih iznad 50, godišnji prihod iznad 10 mil EUR-a)

- **VAŽNI SUBJEKTI** – svi ostali operatori

NADLEŽNA TIJELA

- **HAKOM** - nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti za pružatelje javnih elektroničkih komunikacijskih mreža i usluga

- **Nacionalni centar za kibernetičku sigurnost (SOA) –** središnje državno tijelo za kibernetičku sigurnost, nadležni CSIRT za pružatelje javnih elektroničkih komunikacijskih mreža i usluga

- U slučaju da za pojedini subjekt postoji nadležnost dva ili više tijela, radi izbjegavanja dupliciranja i preklapanja u obavljanju poslova, središnje državno tijelo za kibernetičku sigurnost u suradnji sa svim tijelima nadležnim za subjekt izrađuje protokol o postupanju nadležnih tijela, vodeći računa primarno o glavnoj djelatnosti subjekta

KATEGORIZACIJA

- **HAKOM** provodi kategorizaciju za telekom sektor

- rok za provođenje kategorizacije – godina dana od dana stupanja na snagu ZKS-a
- Postupak kategorizacije obuhvaća i postupak nacionalne procjene kibernetičkog rizika operatora sukladno kalkulatoru za izračun razine kibernetičkog rizika (izrađuje SDTKS-SOA-90 dana nakon stupanja Uredbe na snagu
- Moguće razine KS rizika : niska, srednja i visoka (osnovne, srednje i napredne mjere iz Priloga II Uredbe)

MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

Uključuju:

- politike analize rizika i sigurnosti informacijskih sustava
- postupanje s incidentima
- kontinuitet poslovanja
- sigurnost lanca opskrbe
- osnovne prakse kibernetičke higijene
- sigurnost ljudskih resursa, politike kontrole pristupa i dr.…

Prilog II Uredbe o kibernetičkoj sigurnosti

MJERE UPRAVLJANJA KIBERNETIČKIM SIGURNOSNIM RIZICIMA

- Ključni i važni subjekti – dužni su provesti mjere upravljanja kibernetičkim sigurnosnim rizicima u roku od godine dana od dana kada zaprime obavijest o kategorizaciji
- Za provedbu mjera – odgovorni su članovi upravljačkih tijela
- Provjera usklađenosti:
    - postupak **revizije** kibernetičkih sigurnosti ključnih i važnih subjekata
    - postupak **samoprocjene** kibernetičke sigurnosti važnih subjekata

POSEBNE MJERE FIZIČKE SIGURNOSTI

- Prilog III Uredbe o kibernetičkoj sigurnosti :

Posebne mjere fizičke sigurnosti za subjekte iz sektora digitalne infrastructure (što uključuje i telekom sektor)

- odnos s CER Direktivom

REVIZIJA I SAMOPROCJENA

- reviziju odnosno samoprocjenu subjekti su dužni provoditi najmanje jednom u dvije godine (+ na zahtjev nadležnog tijela) – rok počinje teći nakon isteka roka od godine dana od dana zaprimanja obavijesti o kategorizaciji
- troškove snose ključni i važni subjekti
- samoprocjena – važni subjekti mogu koristiti i vanjskog davatelja takve usluge
- Uredba o kibernetičkoj sigurnosti – pravila, tehnički zahtjevi, norme, obrasci i postupci koji se primjenjuju prilikom samoprocjene kibernetičke sigurnosti

OBAVJEŠTAVANJE O INCIDENTIMA

- ključni i važni subjekti dužni su u roku od 30 dana od dana zaprimanja obavijesti o kategorizaciji započeti s obavjštavanjem o incidentima
- Obavještava se CSIRT - Nacionalni centar za kibernetičku sigurnost (SOA)
- Kriteriji za utvrđivanje značajnih incidenata – propisani su Uredbom o kibernetičkoj sigurnosti

STRUČNI NADZOR

- stručni nadzor nad provedbom zahtjeva kibernetičke sigurnosti provode inspektori HAKOM-a
- ključni subjekti – jednom u roku od 3 do 5 godina (rok se računa nakon proteka 1 godine od kad je subjekt zaprimio obavijest o kategorizaciji) - IZNIMNO i ranije
- važni subjekti – kad nadležno tijelo raspolaže informacijom da subjekt ne ispunjava obveze

KOREKTIVNE MJERE i PREKRŠAJI

- Korektivne mjere – upozorenja, upute, nalozi

- Posebne korektivne mjere za ključne subjekte:
  -privremene suspenzije – zabrana obavljanja upravljačkih dužnosti u ključnom subjektu
  -zabrane obavljanja djelatnosti

- Ovlašteni tužitelj za telekom sektor je HAKOM

Traju dok ključni subjekt ne postupi u skladu s izrečenim korektivnim mjerama.

NAKON DONOŠENJA ZKS UREDBE POTREBNO JOŠ...

- Središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti donosi pravila za provedbu samoprocjena kibernetičke sigurnosti, čiji su sastavni dio opisi razina zrelosti kibernetičke sigurnosti i pripadni kalkulator za bodovanje i izračun stupnja usklađenosti uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima i trenda podizanja razine zrelosti kibernetičke sigurnosti subjekta te obrazac izjave o sukladnosti (ZSIS na svojim web stranicama u roku od 6 mjeseci od dana stupanja na snagu Uredbe)
- Nadležni CSIRT-ovi će donijeti smjernice koje će propisati obrazce izvještavanja o značajnim incidentima - u roku od 90 dana od dana stupanja na snagu ove Uredbe
- Središnje državno tijelo za kibernetičku sigurnost donijet će nacionalnu taksonomiju incidenata - u roku od 90 dana od dana stupanja na snagu ove Uredbe.
- Na stranicama SOA-e će biti:
  - kalkulator KS procjene rizika-u roku 90 dana,
  - smjernice kojima se pojašnjava provedba mjere naziva „Upravljanje rizicima“ i pregled međunarodnih standard- u roku 6 mjeseci

Hvala na pažnji!

Vesna Gašpar i Jagoda Peleponjko

vesna.gaspar@hakom.hr

jagoda.peleponjko@hakom.hr