PREDLOG!

Na podlagi sedmega odstavka 115. člena Zakona o elektronskih komunikacijah –ZEKom-2 (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O) izdaja Agencija za komunikacijska omrežja in storitve Republike Slovenije

SPLOŠNI AKT
o varnosti omrežij, storitev in podatkov

I. SPLOŠNE DOLOČBE

1. člen
(vsebina splošnega akta)

Ta splošni akt podrobneje določa vsebino in strukturo varnostne dokumentacije, usmeritve glede obravnave tveganj, minimalni obseg in vsebino varnostnih ukrepov, usmeritve glede načrtovanja in zagotavljanja neprekinjenega poslovanja ter dodatne varnostne zahteve za operaterje mobilnih komunikacijskih omrežij.

2. člen
(pomen izrazov)

(1) Izrazi, uporabljeni v tem splošnem aktu, pomenijo:

1. Avtentičnost je pristna in nepotvorjena lastnost omrežja, shranjenih, obdelanih ali prenesenih komunikacijskih in meta podatkov in entitet kot se izkazuje (npr. uporabniku, procesu ali sistemu).

2. Celovitost omrežja je zmožnost sistema, da zagotovi določene lastnosti v okviru vnaprej opredeljenih zmogljivosti in funkcionalnosti z namenom, da se zagotovi neprekinjeno delovanje oziroma razpoložljivost.

3. Grožnja je potencialna nevarnost ozirom možen vzrok za varnostni incident, ki bi lahko ob primernih okoliščinah povzročila škodo organizaciji oziroma negativno vplivala na zaupnost, celovitost in razpoložljivost sredstva ali skupine sredstev.

4. Kibernetska grožnja je grožnja skladno z zakonom, ki ureja informacijsko varnost.

5. Kritična sredstva so sredstva, ki vključujejo elemente, funkcije ter storitve omrežja ter podporni informacijski sistemi v fizični, programski ali kakršni koli virtualizirani obliki pri operaterju ali pri ponudniku storitev v oblaku, ki operaterju takšne storitve zagotavlja, katerih potencialna odpoved ali zloraba bi lahko imela zelo velik negativni vpliv na varnost in nemoteno delovanje storitev kritičnih subjektov ali na varnost in nemoteno delovanje zasebnih omrežij kritičnih subjektov ali bi kako drugače pomembno ogrozila

vitalne gospodarske ali družbene aktivnosti države oziroma bi lahko ogrozilo tudi nacionalno varnost.

6. Kritični subjekti so upravljavci kritične infrastrukture skladno z zakonom, ki ureja kritično infrastrukturo, izvajalci bistvenih storitev, organi državne uprave in ostali zavezanci na podlagi zakona, ki ureja informacijsko varnost in nosilci ključnih delov sistema varnosti države.

7. Ranljivost je obstoj šibkosti arhitekture ali posamezne opreme, procesov, posledica napak v implementaciji ali upravljanju, odsotnosti notranjih kontrol, ki lahko vodi v nepričakovane neželene dogodke, ki lahko ogrozijo varnost omrežij, komunikacijskih protokolov, aplikacij in storitev.

8. Razpoložljivost pomeni pravočasen in zanesljiv dostop do sredstev, omrežij, podatkov ali informacij na zahtevo pooblaščene entitete.

9. Nacionalni CISRT pomeni nacionalno skupino za obravnavanje incidentov v skladu z zakonom, ki ureja informacijsko varnost.

10. Sredstvo je vse kar ima določeno vrednost za organizacijo, predvsem pa vključuje strojno in programsko opremo, podatke, mrežno infrastrukturo in ljudi.

11. Tveganje je potencial oziroma verjetnost, da bo dana grožnja izkoristila ranljivost sredstva ali skupine sredstev in tako povzročila organizaciji škodo oziroma negativno vplivala na zaupnost, celovitost in razpoložljivost sredstev ali skupne sredstev.

12. Zaupnost je lastnost shranjenih, prenesenih ali obdelanih podatkov in povezanih storitev, ki zagotavlja, da informacija ni na voljo ali razkrita nepooblaščenim osebam ali procesom.

(2) Preostali izrazi, uporabljeni v tem splošnem aktu, imajo enak pomen kot je določen v Zakonu o elektronskih komunikacijah – ZEKom-2 (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O; v nadaljnjem besedilu: ZEKom-2).

II. SISTEM UPRAVLJANJA VAROVANJA INFORMACIJ IN NEPREKINJENEGA POSLOVANJA

3. člen
(vsebina Sistema upravljanja varovanja informacij)

(1) Operater opredeli obseg in meje Sistema upravljanja varovanja informacij (v nadaljnjem besedilu: SUVI) z namenom, da v kontinuiranem procesu prepoznava in uspešno obvladuje vsa ključna zunanja in notranja tveganja, ki bi lahko pomembno ogrozila varnost informacij, varnost oziroma neprekinjeno delovanje omrežja, pripadajočih informacijskih sistemov ali storitev, pri čemer upošteva določila VIII. poglavja ZEKom-2.

(2) Poleg zahtev, navedenih v tretjem odstavku 115. člena ZEKom-2, SUVI zajema najmanj še:

1. navedbo uporabljene metodologije in orodij, s katerimi se izvajajo analize tveganj,
2. opredelitev in popis vseh sredstev (vključno z nastavitvami), ki so bistvenega pomena za nemoteno in varno delovanje javnih komunikacijskih storitev operaterja,
3. opredelitev in dokumentacijo ključnih poslovnih procesov in stopnjo kritičnosti glede na njihov vpliv na varnost omrežij, informacijskih sistemov, zagotavljanje storitev in varstvo zasebnosti,
4. opredelitev in popis varnostnih tveganj znotraj operaterja in tistih zunaj operaterja glede na sredstva, ki jih uporablja ter glede na storitve, ki jih zagotavlja oziroma najema, in lahko ogrozijo delovanje in varnost javnega komunikacijskega omrežja in storitev,
5. opredelitev in popis varnostnih tveganj znotraj operaterja in tistih zunaj operaterja, ki lahko vplivajo na nepooblaščeno razkritje osebnih in prometnih podatkov in bi to lahko imelo negativen vpliv na zasebnost naročnika ali posameznika,
6. opredelitev verjetnosti nastanka kršitve informacijske varnosti oziroma varnostnega incidenta za vsa opredeljena varnostna tveganja,
7. opredelitev stopnje potencialnih negativnih učinkov in posledic v primeru izrabe ranljivosti ali nerazpoložljivosti vseh sredstev iz 2. točke tega odstavka,
8. opredelitev stopnje potencialnih negativnih učinkov in posledic v primeru izrabe ranljivosti ali nerazpoložljivosti sredstev iz 4. točke tega odstavka,
9. določitev in obrazložitev sprejemljive ravni tveganj iz 4. in 5. točke tega odstavka,
10. popis ukrepov ter načrtov za preprečevanje varnostnih incidentov oziroma za omilitev posledic varnostnega incidenta,
11. popis organizacijskih vlog, odgovornosti in pooblastil znotraj operaterja, pomembnih za varnost omrežij, informacijskih sistemov, podatkov ter fizično varovanje objektov in naprav,
12. jasna načela kadrovske politike in seznam konkretnih pogojev in zahtev za zaposlene na delovnih mestih, ključnih za zagotavljanje varnosti komunikacijskih omrežij in storitev.

(3) Operater odpravlja ugotovljene pomanjkljivosti in neskladnosti SUVI ter nenehno izboljšuje njegovo ustreznost, zadostnost, uspešnost in učinkovitost.

(4) Operater posreduje SUVI oziroma omogoči vpogled agenciji na njeno zahtevo.

4. člen
(minimalni obseg varnostne politike)

(1) Operater pri načrtovanju, izvajanju, spremljanju in izboljševanju informacijske varnostne politike ter pripadajočih ukrepov zajame zlasti:

1. upravljanje s tveganji, opredelitev vlog in odgovornosti v zvezi z izvajanjem varnostne politike tudi v odnosih z zunanjimi izvajalci pri vzpostavitvi, vzdrževanju in nadgradnjah omrežij in informacijskih sistemov,
2. upravljanje s tveganji, povezanimi s kadrovanjem, za namen obvladovanja informacijske varnosti,
3. fizično in logično varnost sredstev, vključno z obvladovanjem dostopnih pravic, zagotavljanjem celovitosti omrežij in informacijskih sistemov, zaščito osebnih in prometnih podatkov ter oskrbo z električno energijo in drugimi energenti,

4. operativne postopke, ki vključujejo upravljanje s sredstvi,
5. prepoznavanje, obvladovanje in poročanje varnostnih incidentov skladno s splošnim aktom, ki ureja poročanje in vrednotenje varnostnih incidentov,
6. zagotavljanje zanesljivosti dobavnih verig, vključno z vidiki povezanimi z varnostjo oziroma dodatnimi varnostnimi zahtevami na podlagi splošnega akta, ki ureja dodatne varnostne zahteve in omejitve,
7. zagotavljanje neprekinjenega poslovanja, ki vključuje upravljanje z varnostnimi kopijami, zagotavljanje podvojenih oziroma nadomestnih elementov omrežja in sistemov in vnovična vzpostavitev delovanja po nepredvidljivih dogodkih, ter obvladovanje kriz,
8. izobraževanje in usposabljanje zaposlenih na področju kibernetske varnosti,
9. nadzorovanje in preizkušanje uvedenih ukrepov v zvezi z zagotavljanjem varnosti, vključno z izvajanjem vdornih testov, zaznavanjem, upravljanjem in poročanjem groženj.

(2) Operater skrbi, da se področja upravljanja z informacijsko varnostjo navedena v prvem odstavku tega člena upoštevajo in izvajajo v skladu z uveljavljenimi nacionalnimi, mednarodnimi in evropskimi standardi (ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27005:2018, ISO/IEC 27035-1:2016, ISO/IEC 27036-3:2013, ISO/IEC 31000:2009, ISO/IEC 22301:2019), praksami in priporočili stroke Agencije Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: ENISA), Skupine za sodelovanje glede varnosti omrežij in informacij (v nadaljnjem besedilu: NIS Cooperation Group) ter zakonodajnimi okviri.

(3) Sprejeti ukrepi iz prvega odstavka tega člena morajo temeljiti na pristopu upoštevanja vseh tveganj, katerih namen je varnost omrežja in informacijskih sistemov in podatkov ter njihovo fizično okolje pred incidenti.

(4) Operater dokumentira sprejete in izvedene ukrepe iz prvega odstavka tega člena in jih predloži na vpogled ali posreduje agenciji na njeno zahtevo.

5. člen
(obravnava in ocenjevanje groženj in ranljivosti)

(1) Operater proaktivno z uporabo dobrih praks, s tehničnimi sredstvi in z dostopnimi viri informacij in podatkovnih zbirk vseskozi prepoznava, obravnava, ocenjuje in vrednoti potencialne grožnje in ranljivosti omrežij, informacijskih sistemov in programske opreme vključno s kibernetskimi grožnjami.

(2) Operater glede na vire, ki jih uporablja za zagotavljanje storitev, obravnava vsaj naslednja tveganja, ki lahko ogrozijo varnost omrežij, informacijskih sistemov in podatkov:
1. tveganja zaradi odpovedi ali napačnega delovanja strojne opreme,
2. tveganja, ki izhajajo iz dobavnih verig,
3. tveganja, ki lahko nastanejo pri oskrbi, vključno v primeru prekinitev ali motenj dobave rezervnih delov ali energentov,
4. tveganja pri uporabi storitev zunanjih ponudnikov oziroma izvajalcev,
5. okoljska tveganja (npr. poplave, požari, žled, potresi, elektromagnetna sevanja),

6. tveganja pri uporabi virtualizacijskih tehnologij, ne glede na tip in vrsto uporabe pri operaterju ali pri ponudniku storitev v oblaku, vključno glede uporabe programsko definiranih omrežjih (SDN),
7. tveganja pri uporabi varnostno neprimerne ali neposodobljene programske ali strojne opreme pri dostopu do omrežja, informacijskih sistemov in storitev,
8. tveganja pri uporabi prosto dostopne programske opreme, vključno v obliki kontejnerjev in mikroservisov,
9. tveganja v zvezi z zlonamernimi dejanji zaradi ranljivosti na področju signalizacije (npr. SS7, Diameter, GTP-C, HTTP2/JSON),
10. tveganja povezana s kibernetskimi grožnjami (npr. zlonamerna in izsiljevalska programska koda, napadi, vdori, prisluškovanje in sleparjenje, prestrezanje in odtekanje podatkov, lažno predstavljanje in kraja identitete, nepooblaščeni dostopi, zlonamerne spremembe nastavitev omrežja in informacijskih sistemov),
11. tveganja na področju izmenjave in usmerjanja prometa,
12. operativna tveganja,
13. tveganja v zvezi z zlorabo oddaljenega dostopa,
14. tveganja izpostavljenih odprtih vmesnikov (API) in storitev,
15. tveganja v zvezi z namernimi in nenamernimi človeškimi dejanji, ki povzročijo uničenje ali škodo omrežju ali informacijskemu sistemu,
16. pravna in poslovna tveganja.

(3) Operater redno obravnava in ocenjuje aktualne grožnje, odpravlja ranljivosti, ter posodablja varnostne ukrepe.

6. člen
(vsebina Sistema upravljanja neprekinjenega poslovanja)

(1) Operater v okviru načrtovanja in izvajanja Sistema upravljanja neprekinjenega poslovanja (v nadaljevanjem besedilu: SUNP), ob upoštevanju lokacij, velikosti, odgovornosti in kompleksnosti organizacije:

1. pripravi dobro dokumentirano strategijo, načrte in postopke za zagotavljanje kontinuitete delovanja in razpoložljivosti omrežja in informacijskih sistemov, podatkov in storitev, ki jih ponuja, da se v primeru naravnih nesreč in drugih nepredvidenih dogodkih po prioritetni ravni omogoči hitro in učinkovito obnovo na sprejemljivi, vnaprej določeni ravni,
2. določi kompetentno osebje, ki izvaja SUNP z jasnimi vlogami, pooblastili in odgovornostmi,
3. pripravi in periodično preverja učinkovitost načrtovanih ukrepov za ključne sisteme, ki se aktivirajo ob nepredvidljivih dogodkih,
4. pripravi in periodično preverja učinkovitost načrtovanih ukrepov ob nepredvidljivih dogodkih za odvisne in soodvisne kritične sektorje, storitve in dobavitelje, od katerih je odvisno delovanje njegovih omrežij, sistemov in storitev,
5. v naprej pripravi in testira primernost potrebnih nadomestnih prostorov, sistemov in elementov omrežja in podpornih sistemov,
6. vzpostavi učinkovit proces shranjevanja oziroma varnostnega arhiviranja (po potrebi na potresno varno rezervno lokacijo) in obnove podatkov v primeru izgube ali zlorabe, ki se periodično preverja,

7. izdela načrt kriznega upravljanja v primeru izpada posameznih lokacij, odpovedi informacijskih sistemov ali posameznih elementov omrežja, izpada oskrbe z električno energijo, drugimi viri, oziroma odpovedjolastnih ali zunanjih storitev,
8. izdela načrt obnove v normalno poslovanje ob motenem ali prekinjenem poslovanju,
9. periodično pregleduje izvajanje ukrepov, analizira pretekle motnje ali prekinitve in zbira podatke o preventivno izvedenih vajah ter skladno z njimi posodablja SUNP.

(2) Za zagotovitev odpornosti omrežij in upravljanje neprekinjenega poslovanja na nacionalni ravni operater vzpostavi in vzdržuje ustrezne zmogljivosti, ukrepe in dogovore z drugimi operaterji, da se zagotovi izvajanje skladno z določili 124. člena ZEKom-2.

(3) Vodstvo operaterja enkrat letno potrdi ustreznost in učinkovitost SUNP. Operaterji dokumentirajo sprejete in izvedene postopke in ukrepe iz prvega odstavka tega člena in jih na njeno zahtevo posredujejo agenciji.

(4) Operater pri pripravi in izvajanju SUNP v največji meri upošteva uveljavljene mednarodne standarde, priporočila stroke in dobre prakse.

7. člen
(upravljanje omrežja, nadzor dostopa do omrežja, informacijskih sistemov in podatkov ter shranjevanje in obdelava podatkov)

(1) Operater pri dostopu do omrežja, informacijskih sistemov in podatkov zagotovi stroga pravila dostopa predvsem tako, da:
1. imajo dostop do omrežja, sistemov, storitev in podatkov le pooblaščeni ter predhodno overjeni in avtorizirani uporabniki,
2. je uporabnikom za dostop do storitev in sistemov dodeljen le unikatni identifikator,
3. je izbran ustrezen avtentikacijski mehanizem glede na vrsto in občutljivost dostopa,
4. se za dostop do ključnih sredstev pri oddaljenem dostopu oziroma dostopu z administracijskimi pravicami in dostopu s strani tretjih oseb vedno uporablja večfaktorsko overjanje in druge ustrezne mehanizme, ki zmanjšujejo verjetnost zlorabe,
5. so jasno opredeljene in dokumentirane vloge, pravice, odgovornosti ter postopki za dodeljevanje in preklic pravic dostopa,
6. se upravičenost dostopnih pravic periodično preverja in posodablja še posebej pri dostopu do ključnih sredstev,
7. se uporablja le odobreno in varnostno preverjeno opremo,
8. so gesla shranjena z nepovratno kriptografsko funkcijo,
9. se vsi dostopi neizbrisno beležijo in hranijo šest mesecev,
10. so vzpostavljeni ustrezni tehnični in organizacijski ukrepi za prepoznavanje in obravnavo kršitev varnostne politike.

(2) Operater zagotovi, da se vsa kritična sredstva ter osebni in prometni podatki nahajajo na območju Republike Slovenije oziroma na ozemlju, držav, ki jih dovoljuje nacionalna in evropska zakonodaja.

8. člen
(varnostna dokumentacija)

(1) Operater pripravi, vodi in redno posodablja najmanj naslednje zapise:
1. v zvezi z obravnavanjem tveganj in vrednotenjem uspešnosti SUVI skladno s 3. členom tega splošnega akta, in sicer:
   a. ažuren načrt fizične in logične arhitekture omrežja ter fizičnih in logičnih povezav z drugimi operaterji,
   b. ažuren seznam izvajanja posodobitev in sprememb (konfiguracij) programske opreme,
   c. ažuren seznam in opis elektronskih komunikacijskih storitev, ki jih operater zagotavlja,
   d. ažuren seznam vseh informacijskih in komunikacijskih sredstev, ki so potrebna za nemoteno delovanje storitev operaterja, njihove skrbnike in upravljalce sredstev, lokacijo sredstev ter vrednotenje sredstev glede na pomembnost in kritičnost funkcije, ki jo sredstvo zagotavlja oz. število in vrsto potencialno prizadetih uporabnikov v primeru odpovedi sredstva ali izrabe njegove ranljivosti,
   e. zapise o okvarah in kršitvah informacijske varnosti,
2. sprejeto varnostno politiko skladno s 4. členom tega splošnega akta,
3. prepoznane grožnje in metodologijo ocenjevanja in upravljanja tveganj skladno s 5. členom tega splošnega akta,
4. popis procesov in operativnih postopkov in njihovo izvajanje skladno s prvim odstavkom 5. člena tega splošnega akta,
5. sprejeto politiko neprekinjenega poslovanja in cilje organizacije skladno s 6. členom tega splošnega akta,
6. vloge in odgovornosti ključnih zaposlenih, odgovornih za zagotavljanje varnosti in neprekinjenega poslovanja, skladno s 6. členom tega splošnega akta,
7. zapise o presojah in vodstvenih pregledih ter sprejetih korektivnih ukrepih skladno s 6. členom tega splošnega akta.
8. ažuren seznam dodeljenih pravic dostopa do omrežnih elementov, sistemov in podatkov skladno s 7. členom tega splošnega akta
9. zapise o aktivnostih uporabnikov, sistemskih administratorjev skladno s 7. členom tega splošnega akta,
10. seznam dobaviteljev za kritična sredstva in varnostno politiko v zvezi z njimi,
11. zapise o incidentih ter sprejetih korektivnih ukrepih kot je to določeno v splošnem aktu, ki ureja o poročanje in vrednotenje varnostnih incidentov

(2) Za dokumente iz prejšnjega odstavka mora operater vzpostaviti dokumentni sistem, ki zagotavlja:
1. odobritev dokumentov, preden so objavljeni,
2. pregledovanje in dopolnjevanje dokumentov,
3. uporabo najnovejših verzij ustreznih dokumentov,
4. da bodo dokumenti na razpolago tistim, ki jih potrebujejo oziroma morajo biti z njimi seznanjeni ter
5. sledljivost in varno hrambo.

9. člen
(varnost omrežij 5G)

(1) Ne glede določbe prvega odstavka 4. člena tega splošnega akta, operater ki upravlja z elementi in funkcijami omrežja 5G še dodatno upošteva, da:

1. elementi in funkcije omrežja 5G izpolnjujejo funkcionalnosti in tehnične specifikacije, kot jih opredeljujejo 3GPP standardi,
2. je zasnova in varnost omrežja 5G in njenih funkcij, izvedena v skladu s priporočili ENISA in Združenja GSMA (v nadaljnjem besedilu: GSMA),
3. pri pripravi ukrepov upošteva ranljivosti, potencialne grožnje in zlonamerne akterje, kot so navedeni v dokumentu NIS Cooperation Group Usklajena ocena tveganja za kibernetsko varnost omrežij 5G (angl. »EU Coordinated risk assessment of the cybersecurity of 5G networks , report 9«, oktober 2019)
4. upošteva industrijske dobre prakse in priporočila ENISA v zvezi z varnostjo omrežij 5G kot so navedene v dokumentih ENISA »5G Supplement – to the Guideline on Security Measures under EECC« (7. julij 2021) in »Security in 5G Specifications – Controls in 3GPP« (24. februar 2021) ter v zvezi z virtualizacijo in virtualiziranimi omrežnimi funkcijami (v nadaljnjem besedilu: NFV, kot so navedene v dokumentu ENISA »NFV Security in 5G – Challanges and Best Practices« (24. februar 2022),
5. je vzpostavljena učinkovita raven upravljanja, nadzora in varnosti omrežja 5G, še posebej pri zaznavanju anomalij, možnih zlorab in nepooblaščenih sprememb na omrežju in storitvenih elementih, znotraj omrežja in s strani končnih naprav,
6. ima dolgoročno strategijo raznolikosti dobavne verige in proizvajalcev opreme, ki upošteva tehnične omejitve in hkrati zagotavlja medsebojno skladnost in nemoteno delovanje,
7. preverja odpornost na ravni fizične obrambe (dostop do objektov in prostorov) in na ravni logične obrambe (testiranje ranljivosti in možnih zlorab na mrežni in aplikativni ravni znotraj in zunaj omrežja operaterja),
8. z namenom zagotavljanja visoke ravni varnosti in preprečevanja zlorab na ravni protokola mejnega prehoda (angl. »Border Gateway Protocol (BGP)) upošteva in izvaja tehnične usmeritve ENISA, kot so navedene v dokumentu ENISA »7 steps to shore up BGP« (maj 2019),
9. z namenom zagotavljanja visoke ravni varnosti na nivoju signalizacije SS7, Diameter, GTP-C, HTTP2/JSON upošteva najnovejši tehnološki razvoj in tehnične usmeritve ENISA kot so navedene v dokumentu »Signalling Security in Telecom SS7/Diameter/5G EU level assessment of the current situation« (marec 2018),
10. prednostno uporablja omrežne komponente 5G ter kriptografski material in profilov (eSIM), ki so prestali presojo v skladu z evropsko certifikacijsko shemo za omrežja 5G (EU5G in SM-UP/SM-DP).

(3) Operater pri načrtovanju ukrepov iz 3., 4., 5., in 8. člena tega splošnega akta sledi dobrim praksam in splošno sprejetimi aktualnim priporočilom stroke, med drugim GSMA in Delovne skupine za internetsko inženirstvo (IETF).

10. člen
(upravljanje tveganj v zvezi z oskrbo električne energije)

(1) Operater z dobavitelji električne energije vzpostavi učinkovit postopek ažurnega obveščanja o morebitnih vzdrževanjih in izpadih dobave električne energije.

(2) Na lokacijah, ki so ključna za delovanje in upravljanje omrežja in informacijskih sistemov operaterja, se mora zagotoviti stalno neprekinjeno napajanje, ki se redno preverja in testira ob delovni obremenitvi.

(3) Operater za vsa večja dostopovna vozlišča ter bazne postaje, ki v vršnih urah zagotavljajo storitve več kot 100 uporabnikom hkrati, zagotavlja vsaj triurno avtonomijo (rezervno napajanje), ki omogoča vsaj delovanje omrežnih priključnih točk s prednostjo, opravljanje storitev komunikacij v sili in govorne komunikacijske storitve na podlagi številke.

(4) Operater vzdržuje popis stanja v zvezi z zagotavljanjem redundantnega napajanja.

(5) Operater sam oziroma v sodelovanju z drugimi operaterji in deležniki pripravi, posodablja in izvaja načrt ukrepanja s prednostnim seznamom lokacij reševanja in obnove storitev v primeru daljšega izpada električne energije.

11. člen
(dodatne varnostne zahteve za operaterje mobilnih komunikacijskih omrežij)

(1) Z namenom, da je vzpostavljena visoka raven varnosti mobilnih komunikacijskih omrežij, operater, ki nudi to omrežje oziroma izvaja storitve za kritične subjekte oziroma ima več kot 100 000 uporabnikov, izvaja SUVI in SUNP v skladu s priznanim mednarodnim ali evropskim standardom, ki obravnavata navedena področja.

(2) Operater dokazuje agenciji skladnost iz prejšnjega člena s predložitvijo izjave o skladnosti periodično v rednih časovnih presledkih, ki niso daljši od treh let.

12. člen
(obravnava varnostnih incidentov in presoja ustreznosti ukrepov)

(1) Agencija operativno sodeluje z nacionalnim CSIRT.

(2) Nacionalni CSIRT nudi pomoč agenciji na njeno utemeljeno zahtevo pri razreševanju in vrednotenju varnostnih incidentov in presoji sprejetih varnostnih ukrepov na strani operaterja.

(3) Agencija po potrebi lahko zaprosi za mnenje in pomoč v zvezi z izvedenimi varnostnimi ukrepi ali rešitvami na strani operaterja tudi drugo usposobljeno neodvisno inštitucijo.

13. člen
(določitev kontaktne osebe)

(1) Operater mora v organizaciji določiti kompetentno in usposobljeno osebo, ki ima pregled nad izvajanjem varnostne politike in ostalih zahtev iz tega splošnega akta v organizaciji.

(2) Operater mora takoj po imenovanju osebe iz prvega odstavka tega člena agenciji na njen uradni naslov oziroma uradni elektronski naslov sporočiti njegove kontaktne podatke in sicer: ime in priimek, navedba funkcije, ki jo opravlja v podjetju, kontaktna telefonska številka, kontaktni elektronski naslov.

14. člen
(notranja in zunanja presoja SUVI in SUNP)

(1) Operater mora najmanj enkrat letno izvesti notranjo presojo SUVI in SUNP (v nadaljnjem besedilu: notranja presoja), kjer ugotavlja primernost, uspešnost in učinkovitost obvladovanja tveganj za varnost omrežij in storitev ter neprekinjenega poslovanja. Načrt izvedbe notranje presoje mora zagotoviti, da se v treh letih od izvedene notranje presoje pregledajo vsi cilji ukrepov, sprejeti ukrepi, procesi in postopki. Notranjo presojo mora opraviti zaposleni, ki ni povezan s področjem, podvrženim presoji. Zaposleni mora za izvajanje tovrstnih pregledov imeti ustrezno znanje in izkušnje.

(2) O rezultatih notranjih presoj je potrebno voditi zapise. Operater mora te zapise hraniti najmanj pet let od posamezne izvedene notranje presoje.

(3) Operater, ki izvaja storitve za izvajalce kritičnih storitev ali ima več kot 100 000 uporabnikov mora v skladu z izbranim standardom vsaka tri leta opraviti tudi zunanjo presojo SUVI in SUNP, ki jo izvede usposobljena organizacija. Operater ugotovitve zunanje presoje vključno z načrtom odpravljanja ugotovljenih nepravilnosti dostavi agenciji do 30. maja za preteklo obdobje presoje.

IV. PREHODNI IN KONČNA DOLOČBA

15. člen
(izjava o skladnosti)

(1) Operater predloži agenciji prvo izjavo o skladnosti v skladu z 11. členom tega splošnega akta v treh letih po uveljavitvi tega splošnega akta.

(2) Operater, ki pisno obvesti agencijo o začetku zagotavljanja javnih komunikacijskih omrežij oziroma izvajanja javnih komunikacijskih storitev v skladu s 5. členom ZEKom-2 po uveljavitvi tega splošnega akta, predloži agenciji prvo izjavo o skladnosti v skladu z 11. členom tega splošnega akta v treh letih od pisnega obvestila.

16. člen
(priprava in zunanja presoja SUVI in SUNP)

(1) Operater pripravi nov SUVI in nov SUNP skladno z zahtevami tega splošnega akta v roku šest mesecev od njegove uveljavitve.

(2) Operater izvede prvo zunanjo presojo SUVI in SUNP v skladu s tretjim odstavkom 14. člena tega splošnega akta v 18 mesecih po uveljavitvi tega splošnega akta.

(3) Operater, ki pisno obvesti agencijo o začetku zagotavljanja javnih komunikacijskih omrežij oziroma izvajanja javnih komunikacijskih storitev v skladu s 5. členom ZEKom-2 po uveljavitvi tega splošnega akta, izvede prvo zunanjo presojo SUVI in SUNP v na podlagi tretjega odstavka 14. člena tega splošnega akta v enem letu od pisnega obvestila.

17. člen
(prenehanje uporabe)

Z dnem uveljavitve tega splošnega akta se preneha uporabljati Splošni akt o varnosti omrežij in storitev (Uradni list RS, št. 75/13, 64/15 in 130/22 – ZEKom-2).

18. člen
(začetek veljavnosti)

Ta splošni akt začne veljati trideseti dan po objavi v Uradnem listu Republike Slovenije.

Št. _____
Ljubljana, dne _____
EVA _____

mag. Tanja Muha
v.d. direktorja