Na podlagi tretjega odstavka 12. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18) minister za javno upravo izdaja

P R A V I L N I K
o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev

I. SPLOŠNE DOLOČBE

1. člen
(vsebina)

Ta pravilnik podrobneje določa vsebino in strukturo varnostne dokumentacije, metodologijo za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov in minimalni obseg ter vsebino varnostnih ukrepov izvajalcev bistvenih storitev.

2. člen
(pomen izrazov)

Izrazi, uporabljeni v tem pravilniku, pomenijo:

1. Celovitost je lastnost informacij, omrežij in informacijskih sistemov, da so točni in popolni.
2. Neprekinjeno poslovanje so aktivnosti, ki so potrebne za ohranjanje poslovanja organizacije v času motenj ali prekinitev normalnega delovanja.
3. Razpoložljivost je lastnost informacij, omrežij in informacijskih sistemov, da so dostopni in uporabni na pooblaščeno zahtevo.
4. Sistem upravljanja neprekinjenega poslovanja je sistem upravljanja, ki temelji na strateški in taktični sposobnosti organizacije, da pripravi načrt za primere prekinitev in motenj pri poslovanju ter se na njih odzove z namenom zagotovitve storitev na sprejemljivi, vnaprej določeni ravni ter vključuje pripravo in uporabo načrtov obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov (v nadaljnjem besedilu: SUNP).
5. Sistem upravljanja varovanja informacij je sistem upravljanja, ki omogoča celovit in koordiniran pogled na informacijska varnostna tveganja organizacije ter zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti omrežij in informacijskih sistemov (v nadaljnjem besedilu: SUVI).
6. Sredstvo je vsaka opredmetena ali neopredmetena stvar, ki ima vrednost za izvajalca bistvenih storitev (v nadaljnjem besedilu: IBS) in ki zato zahteva zaščito.
7. Trajanje incidenta je časovno obdobje od prekinitve ustreznega zagotavljanja storitve v smislu razpoložljivosti, celovitosti ali zaupnosti do trenutka njene ponovne vzpostavitve.
8. Uporabnik je fizična ali pravna oseba, ki uporablja posamezno bistveno storitev neposredno, posredno ali s posredovanjem oziroma je odvisna od nje.
9. Zaupnost je lastnost, da informacije niso razpoložljive ali razkrite nepooblaščenim subjektom ali procesom.

II. VSEBINA IN STRUKTURA VARNOSTNE DOKUMENTACIJE

3. člen
(vsebina in struktura varnostne dokumentacije)

(1) IBS vzpostavijo in vzdržujejo dokumentiran SUVI in SUNP, ki mora obsegati najmanj elemente iz prvega odstavka 12. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18).

(2) Varnostno dokumentacijo iz prejšnjega odstavka podpiše zakoniti zastopnik IBS.

(3) Če ima IBS za zagotavljanje varnosti svojih omrežij in informacijskih sistemov že izdelano varnostno dokumentacijo na podlagi drugih predpisov, jo vsebinsko dopolni v skladu s tem pravilnikom.

4. člen
(analiza obvladovanja tveganj)

Analiza obvladovanja tveganj z oceno sprejemljive ravni tveganj (v nadaljnjem besedilu: analiza obvladovanj tveganj) obsega najmanj:
1. navedbo sredstev znotraj SUVI in upravljavce teh sredstev,
2. navedbo potencialnih groženj tem sredstvom,
3. navedbo ranljivosti sredstev iz 1. točke tega člena, ki bi jih lahko grožnje iz prejšnje točke prizadele,
4. navedbo vpliva uresničitve groženj iz 2. točke tega člena na razpoložljivost, celovitost in zaupnost sredstev iz 1. točke tega člena zaradi ranljivosti iz prejšnje točke,
5. oceno vpliva na opravljanje bistvenih storitev v primeru kršitve informacijske varnosti zaradi izgube razpoložljivosti, celovitosti ali zaupnosti,
6. realistično oceno verjetnosti, da pride do kršitve informacijske varnosti,
7. ovrednotenje ravni tveganj in
8. določitev sprejemljive ravni tveganj.

5. člen
(politika neprekinjenega poslovanja)

Politika neprekinjenega poslovanja z načrtom njegovega upravljanja (v nadaljnjem besedilu: politika neprekinjenega poslovanja) obsega najmanj:
1. navedbo postopkov neprekinjenega poslovanja, ki se jo izdela na podlagi popisa poslovnih procesov,
2. oceno vpliva na poslovanje, ki zajema navedbo možnih dogodkov in incidentov, ki vplivajo na neprekinjeno poslovanje, vključno zaradi odpovedi informacijskih sistemov, pomanjkanja zaposlenih, izpada posamezne lokacije znotraj IBS in odpovedi storitev pogodbenih izvajalcev,
3. določitev minimalne ravni poslovanja,
4. navedbo ukrepov za zagotavljanje neprekinjenega poslovanja, ki se izdela na podlagi ocene vpliva na poslovanje iz 2. točke tega člena in minimalne ravni poslovanja iz prejšnje točke ter
5. določitev vlog in odgovornosti za izvajanje politike neprekinjenega poslovanja in njeno posodabljanje.

6. člen
(seznam ključnih, krmilnih in nadzornih informacijskih sistemov)

Seznam ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja IBS ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev (v nadaljnjem besedilu: ključni, krmilni in nadzorni informacijski sistemi) obsega najmanj:

- navedbo sredstev znotraj SUVI, od katerih je odvisno zagotavljanje bistvenih storitev, in
- opredelitev ključnih, krmilnih in nadzornih informacijskih sistemov in navedbo njihovih upravljavcev.

7. člen
(načrt obnovitve delovanja informacijskih sistemov)

Načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnjega člena (v nadaljnjem besedilu: načrt obnovitve delovanja informacijskih sistemov) zajema opis odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja.

8. člen
(načrt odzivanja na incidente)

(1) Načrt odzivanja na incidente s protokolom obveščanja nacionalnega CSIRT (v nadaljnjem besedilu: načrt odzivanja na incidente) obsega najmanj:
1. opis sistema za zaznavo incidentov informacijske varnosti,
2. opis sistema za zbiranje in zavarovanje dokazov o incidentu informacijske varnosti, vključno z dnevniškimi zapisi in revizijskimi sledmi, če te obstajajo,
3. opis postopkov za odziv, obravnavo in analizo incidentov informacijske varnosti, vključno z beleženjem vseh odzivnih aktivnosti,
4. opis odgovornosti oseb oziroma organizacijskih enot, ki jih je treba vključiti v aktivnosti iz prejšnje točke,
5. opis postopkov in odgovornosti za poročanje o incidentih znotraj IBS in izven IBS ter
6. opis protokola obveščanja nacionalnega CSIRT o incidentu informacijske varnosti.

(2) Obvestilo iz 6. točke prejšnjega odstavka se pošlje nacionalnemu CSIRT na način, kot je objavljen na njegovi spletni strani in zajema najmanj:
1. oceno števila uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvenih storitev,
2. oceno trajanja incidenta,
3. oceno geografske razširjenosti, kar zadeva območje, na katerega incident vpliva,
4. oceno morebitnega čezmejnega vpliva incidenta,
5. oceno morebitnega medpodročnega vpliva incidenta in
6. oceno pomembnosti vpliva incidenta na neprekinjeno izvajanje bistvenih storitev (lažji incident, težji incident, kritični incident).

9. člen
(načrt varnostnih ukrepov)

(1) Pri izdelavi načrta varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov IBS upoštevajo:
- dokumente varnostne dokumentacije iz 4. do 8. člena tega pravilnika in
- posebne potrebe področja, na katerem deluje posamezen IBS.

(2) Načrt varnostnih ukrepov iz prejšnjega odstavka vsebuje navedbo ukrepov, ki so:
1. učinkoviti tako, da povečajo informacijsko varnost glede na obstoječe in predvidene grožnje,
2. prilagojeni tako, da se prizadevanja IBS usmerijo v ukrepe, ki najbolj vplivajo na njihovo informacijsko varnost in se izogibajo podvajanjem,

3. skladni tako, da se primarno obravnavajo osnovne in skupne varnostne ranljivosti IBS kljub področnim posebnostim, ki se lahko dopolnijo z varnostnimi ukrepi za posamezna področja,
4. sorazmerni s tveganji tako, da se izogiba prekomernemu bremenu za IBS,
5. konkretni tako, da IBS te varnostne ukrepe izvajajo in da ti ukrepi prispevajo h krepitvi njihove informacijske varnosti,
6. preverljivi tako, da lahko na zahtevo pristojnega organa predložijo dokazila o njihovi implementaciji,
7. vključujoči tako, da so upoštevani vsi vidiki informacijske varnosti, vključno s fizično varnostjo informacijskih sistemov.

III. METODOLOGIJI ZA PRIPRAVO ANALIZE OBVLADOVANJA TVEGANJ IN ZA DOLOČITEV KLJUČNIH, KRMILNIH IN NADZORNIH INFORMACIJSKIH SISTEMOV TER PRIPADAJOČIH PODATKOV

10. člen
(metodologiji za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov)

(1) IBS analizo obvladovanja tveganj pripravi tako, da:
1. izvede popis sredstev znotraj SUVI in določi njihove upravljavce,
2. prepozna možne grožnje za izgubo celovitosti, razpoložljivosti in zaupnosti sredstev iz prejšnje točke,
3. prepozna ranljivosti sredstev iz 1. točke tega odstavka, ki bi jih lahko grožnje iz prejšnje točke prizadele,
4. oceni stopnjo vpliva uresničitve groženj iz 2. točke tega odstavka na razpoložljivost, celovitost in zaupnost sredstev iz 1. točke tega odstavka zaradi ranljivosti iz prejšnje točke,
5. oceni primernost obstoječih ukrepov in stopnjo obvladovanja ugotovljenih tveganj s temi ukrepi,
6. ovrednoti ugotovljena tveganja glede na verjetnost nastanka tveganj in obseg negativnih posledic ob uresničitvi tveganj na zagotavljanje storitev ter
7. določi oceno sprejemljive ravni tveganja glede na vrednotenje ugotovljenih tveganj.

(2) IBS seznam svojih ključnih, krmilnih in nadzornih informacijskih sistemov pripravi tako, da:
- izmed popisanih sredstev znotraj SUVI iz 1. točke prejšnjega odstavka presodi, ali je zagotavljanje bistvenih storitev odvisno od posameznega sredstva znotraj SUVI, in
- izmed posameznih sredstev znotraj SUVI, od katerih je v skladu s prejšnjo točko odvisno zagotavljanje bistvenih storitev, presodi, katero izmed teh sredstev je bistveno za delovanje bistvene storitve.

(3) IBS izvede analizo obvladovanj tveganj in določi ključne, krmilne in nadzorne informacijske sisteme tako, da bodo rezultati teh postopkov dosledni, primerljivi in verodostojni.

(4) IBS izvaja analizo obvladovanj tveganj ter določa ključne, krmilne in nadzorne informacijske sisteme v rednih časovnih presledkih ali kadar so predlagane ali nastanejo bistvene spremembe v okviru SUVI.

IV. MINIMALNI OBSEG IN VSEBINA VARNOSTNIH UKREPOV

11. člen
(minimalni obseg in vsebina varnostnih ukrepov)

IBS za zagotavljanje celovitosti, zaupnosti ter razpoložljivosti omrežij in informacijskih sistemov na podlagi varnostne dokumentacije iz 3. člena tega pravilnika pripravijo in izvajajo organizacijske, logično-tehnične in tehnične varnostne ukrepe, ki zagotavljajo najmanj:

1. podporo vodstva IBS zagotavljanju informacijske varnosti, vključno z vključevanjem področja informacijske varnosti v letni načrt poslovanja IBS,
2. integriteto kadrov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve,
3. notranjo presojo SUVI in SUNP v rednih časovnih presledkih,
4. upravljanje ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev, z določitvijo ustrezne odgovornosti za njihovo zaščito,
5. ohranjanje dnevniških zapisov o delovanju ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja iz prejšnje točke,
6. upravljanje prometa in komunikacij,
7. opredelitev varnostnih zahtev za ključne dobavitelje IBS,
8. fizično in tehnično varovanje dostopov do prostorov, kjer so ključni, krmilni in nadzorni informacijski sistemi IBS,
9. varnostne mehanizme v posamezni aplikativni programski opremi za izvajanje dejavnosti IBS,
10. preverjanje identitete uporabnikov,
11. upravljanje pooblastil za dostop,
12. zagotavljanje ravni dostopnosti informacij,
13. zaščito pred zlonamerno programsko kodo,
14. beleženje dejavnosti ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov,njihovih uporabnikov in administratorjev ter
15. zaznavanje poskusov vdorov in preprečevanje incidentov.

V. KONČNA DOLOČBA

12. člen
(začetek veljavnosti)

Ta pravilnik začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

Št. 386-18/2018/35
Ljubljana, dne 13. maja 2019
EVA 2018-3130-0031

Rudi Medved
minister
za javno upravo