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

Pravilnik 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)

(1) Izrazi, uporabljeni v tem pravilniku imajo naslednji pomen:

1. Celovitost je lastnost omrežij in informacijskih sistemov, ki zagotavlja nedotaknjenost podatkov, njihovo točnost in popolnost čez celotni življenjski cikel.

2. Neprekinjeno poslovanje je sposobnost organizacije poslovanja, da po incidentu z negativnim vplivom ohrani ali po potrebi ponovno vzpostavi zagotavljanje storitev na sprejemljivih, vnaprej določenih ravneh.

3. Razpoložljivost je lastnost, ki zagotavlja dostop in uporabo informacij in informacijskih sistemov na pooblaščeno zahtevo.

4. Sistem upravljanja neprekinjenega poslovanja je tisti del celotnega sistema 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 tisti del celotnega sistema 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 ali značilnost, 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, avtentičnosti, 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 omrežij in informacijskih sistemov, ki zagotavlja, da shranjeni, preneseni ali obdelani podatki niso razpoložljivi ali razkriti nepooblaščenim subjektom ali procesom.

(2) Drugi izrazi, uporabljeni v tem pravilniku, imajo enak pomen, kot je določen v zakonu, ki ureja informacijsko varnost.

3. člen

(standardi)

Pri izvajanju tega pravilnika IBS z namenom zagotavljanja informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov, s katerimi zagotavljajo izvajanje bistvenih storitev, kar najbolj upoštevajo uveljavljene evropske ali mednarodno sprejete standarde ali specifikacije s področja varnosti omrežij in informacijskih sistemov.

II. VSEBINA IN STRUKTURA VARNOSTNE DOKUMENTACIJE

4. člen
(vsebina in struktura varnostne dokumentacije)

(1) Skladno z zakonom, ki ureja informacijsko varnost, IBS za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja, ki mora obsegati najmanj:
1. analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj (v nadaljnjem besedilu: analiza obvladovanja tveganj);
2. politiko neprekinjenega poslovanja z načrtom njegovega upravljanja (v nadaljnjem besedilu: politika neprekinjenega poslovanja);
3. seznam njegovih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev (v nadaljnjem besedilu: seznam ključnih, krmilnih in nadzornih informacijskih sistemov);
4. načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje alineje (v nadaljnjem besedilu: načrt obnovitve delovanja informacijskih sistemov);
5. načrt odzivanja na incidente s protokolom obveščanja nacionalnega CSIRT (v nadaljnjem besedilu: načrt odzivanja na incidente);

6. načrt varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov, ki upoštevajo področne posebnosti (v nadaljnjem besedilu: načrt varnostnih ukrepov).

(2) Varnostno dokumentacijo iz prejšnjega odstavka tega člena podpiše zakoniti zastopnik IBS skupaj z izjavo, da vodstvo podpira vzpostavitev in vzdrževanje dokumentiranega sistema upravljanja varovanja informacij ter sistema upravljanja neprekinjenega poslovanja.

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

(4) IBS s področja bančništva, katerih zagotavljanje storitev je odvisno od informacijskih sistemov Banke Slovenije, ki niso informacijski sistemi, ki jih upravlja Evropski sistem centralnih bank, ali ki niso informacijski sistemi v upravljanju Banke Slovenije, ki jih nadzira Evropski sistem centralnih bank, in jih Banka Slovenije uporablja za izvajanje svojih nalog po Zakonu o Banki Slovenije (Uradni list RS, št. 72/06 – uradno prečiščeno besedilo, 59/11 in 55/17; v nadaljnjem besedilu ZBS-1) oziroma drugih nacionalnih predpisih, Statutu Evropskega sistema centralnih bank in Evropske centralne banke (UL C št. 326 z dne 26. 10. 2012, str. 230; v nadaljnjem besedilu: Statut) in predpisih Evropske unije, dopolnijo varnostno dokumentacijo glede teh informacijskih sistemov v skladu z zahtevami Banke Slovenije.

(5) Podatki iz prejšnjega odstavka, ki jih ima na voljo Banka Slovenije in so v skladu z ZBS-1, Statutom in drugimi predpisi določeni kot zaupni, se lahko uporabijo le v skladu s temi predpisi.

5. člen
(analiza obvladovanja tveganj)

Analiza obvladovanja tveganj iz 1. točke prvega odstavka prejšnjega člena tega pravilnika obsega najmanj:

1. navedbo sredstev znotraj SUVI in upravljavce teh sredstev,
2. navedbo potencialnih groženj tem sredstvom
3. navedbo ranljivosti sredstev iz prve točke, ki bi jih lahko grožnje iz prejšnje točke prizadele,
4. navedbo vpliva na razpoložljivost, celovitost in zaupnosti v primeru uresničitve groženj iz druge točke na ranljivosti iz prejšnje točke,
5. ocena vpliva na opravljanje bistvenih storitev v primeru kršitve informacijske varnosti zaradi izgube razpoložljivosti, celovitosti ali zaupnosti,
6. realistična ocena možnosti, da pride do kršitve informacijske varnosti,
7. ocena nivoja resnosti tveganj in
8. določitev sprejemljive ravni tveganj.

6. člen
(politika neprekinjenega poslovanja)

Politika neprekinjenega poslovanja iz 2. točke prvega odstavka 4. člena tega pravilnika obsega najmanj:

1. navedbo postopkov neprekinjenega poslovanja, ki se jo izdela na podlagi popisa poslovnih procesov,
2. ocene vpliva na poslovanje, ki zajema navedbo možnih dogodkov in incidentov, ki vplivajo na neprekinjeno poslovanje, vključno zaradi odpovedi informacijskih sistemov, pomanjkanja zaposlenih, izpada lokacije in odpovedi storitev pogodbenih sodelavcev,
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.

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

Seznam ključnih, krmilnih in nadzornih informacijskih sistemov iz 3. točke prvega odstavka 4. člena tega pravilnika obsega najmanj:

- navedbo sredstev znotraj SUVI, od katerih je odvisno zagotavljanje bistvenih storitev, in
- seznam ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev, in navedbo njihovih upravljavcev.

8. člen
(načrt obnovitve delovanja informacijskih sistemov)

Načrt obnovitve delovanja informacijskih sistemov iz 4. točke prvega odstavka 4. člena tega pravilnika zajema opis odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja.

9. člen
(načrt odzivanja na incidente)

(1) Načrt odzivanja na incidente iz 5. točke prvega odstavka 4. člena obsega najmanj:
- opis sistema za zaznavo incidentov informacijske varnosti,
- opis sistema za zbiranje in zavarovanje dokazov o incidentu informacijske varnosti, vključno z dnevniškimi zapisi in revizijskimi sledmi, če te obstajajo,
- opis postopkov za odziv, obravnavo in analizo incidentov informacijske varnosti, vključno z beleženjem vseh odzivnih aktivnosti,
- opis odgovornosti oseb oziroma organizacijskih enot, ki jih je potrebno vključiti

v aktivnosti iz prejšnje alineje,
- opis postopkov in odgovornosti za poročanje o incidentih notranjim ali zunanjim osebam ali organizacijam in
- opis protokola obveščanja nacionalnega CSIRT o incidentu informacijske varnosti.

(2) Obvestilo nacionalnemu CSIRT iz zadnje alineje prejšnjega odstavka zajema najmanj:
- oceno števila uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvenih storitev,
- oceno trajanja incidenta,
- oceno geografske razširjenosti, kar zadeva območje, na katerega incident vpliva,
- oceno morebitnega čezmejnega vpliva incidenta,
- oceno morebitnega medpodročnega vpliva incidenta in
- oceno pomembnosti vpliva incidenta na neprekinjeno izvajanje bistvenih storitev (lažji incident, težji incident, kritični incident).

10. člen
(načrt varnostnih ukrepov)

(1) Pri izdelavi načrta varnostnih ukrepov iz 6. točke prvega odstavka 4. člena tega pravilnika za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov IBS upoštevajo:
- dokumente varnostne dokumentacije od vključno 4. do 9. 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 sedanje in predvidene grožnje,
2. prilagojeni tako, da se prizadevanja IBS usmerijo v ukrepe, ki najbolj vplivajo na njihovo informacijsko varnost ter v izogib nepotrebnim prizadevanjem in podvajanjem,
3. združljivi tako, da se najprej obravnavajo osnovne in skupne varnostne ranljivosti IBS kljub področnim posebnostim, ki se lahko medtem dopolnijo z varnostnimi ukrepi za posamezna področja,
4. sorazmerni s tveganji v izogib prekomernemu bremenu za IBS,
5. konkretni tako, da je jasno zaznavno, da IBS te varnostne ukrepe dejansko izvajajo in da ti ukrepi dejansko prispevajo k 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. METODOLOGIJA ZA PRIPRAVO ANALIZE OBVLADOVANJA TVEGANJ IN ZA DOLOČITVE KLJUČNIH, KRMILNIH IN NADZORNIH INFORMACIJSKIH SISTEMOV TER PRIPADAJOČIH PODATKOV

11. člen
(metodologija 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 iz 5. člena tega pravilnika pripravi na način, da:

1. izvede popis sredstev znotraj SUVI in določi njihove upravljavce,
2. prepozna možne grožnje, tveganja in dejavnike tveganja, povezana z izgubo celovitosti, razpoložljivosti in zaupnosti informacij znotraj SUVI,
3. oceni primernost obstoječih ukrepov za obvladovanje ugotovljenih tveganj,
4. oceni stopnjo obvladovanja ugotovljenih tveganj glede na primernost obstoječih ukrepov za obvladovanje tveganj,
5. ovrednoti ugotovljena tveganja glede na verjetnost nastanka tveganj in obseg negativnih posledic ob uresničitvi tveganj na zagotavljanje storitev in
6. naredi oceno sprejemljive ravni tveganja glede na vrednotenje ugotovljenih tveganj.

(2) IBS seznam svojih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov iz 7. člena tega pravilnika, ki so bistvenega pomena za delovanje bistvenih storitev, pripravi na način, da:

- izmed popisanih sredstev znotraj SUVI iz prve točke prejšnjega odstavka presodi, ali je zagotavljanje bistvenih storitev odvisno od posameznega sredstva znotraj SUVI, in
- izmed posameznih sredstev znotraj SUVI, od katerih je skladno s prejšnjo alinejo 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 in dele omrežja ter pripadajoče podatke tako, da bodo rezultati teh postopkov dosledni, primerljivi in veljavni.

(4) IBS izvaja analizo obvladovanj tveganj ter določa ključne, krmilne in nadzorne informacijske sisteme in dele omrežja ter pripadajoče podatke v rednih časovnih presledkih ali kadar so predlagane ali nastanejo bistvene spremembe v okviru sistema upravljanja informacijske varnosti.

IV. MINIMALNI OBSEG IN VSEBINA VARNOSTNIH UKREPOV

12. člen
(minimalni obseg in vsebina varnostnih ukrepov)

(1) IBS za zagotavljanje celovitosti, zaupnosti, razpoložljivosti omrežij in informacijskih sistemov na podlagi varnostne dokumentacije iz 4. člena tega pravilnika pripravijo in izvajajo organizacijske, logično-tehnične in tehnične varnostne ukrepe.

(2) Organizacijsko varnostni ukrepi iz prejšnjega odstavka obsegajo najmanj:

- podporo vodstva IBS zagotavljanju informacijske varnosti, vključno z vključevanjem področja informacijske varnosti v letni načrt poslovanja IBS,
- zagotavljanje integritete človeških virov v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo ter ob prenehanju ali spremembi zaposlitve,
- zagotavljanje upravljanja ključnih, krmilnih in nadzornih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev z določitvijo ustrezne odgovornosti za zaščito teh sistemov,
- opredelitev načina ustreznega ohranjanja dnevniških zapisov o delovanju ključnih, krmilnih ali nadzornih informacijskih sistemov in delov omrežja iz prejšnje točke,
- upravljanje prometa in komunikacij in
- opredelitev varnostnih zahtev za ključne dobavitelje.

(3) Logično-tehnični varnostni ukrepi iz prvega odstavka tega člena obsegajo najmanj:

- zagotavljanje fizičnega in tehničnega varovanja dostopov do prostorov, kjer se nahajajo ključni, krmilni ali nadzorni informacijski sistemi IBS,
- zagotavljanje mehanizmov za varnost v posamezni aplikativni programski opremi za izvajanje dejavnosti zavezanca.

(4) Tehnično varnostni ukrepi iz prvega odstavka tega člena obsegajo najmanj:

1. uporabo orodij za preverjanje identitete uporabnikov,
2. uporabo orodij za upravljanje pooblastil za dostop,
3. uporabo orodij za zagotavljanje ravni dostopnosti informacij,
4. uporabo orodij za zaščito pred zlonamernimi kodami,
5. uporabo orodij za beleženje dejavnosti ključnih, krmilnih in nadzornih sistemov in delov omrežja ter pripadajočih podatkov, njihovih uporabnikov in administratorjev ter
6. uporabo orodij za zaznavanje poskusov vdorov in preprečevanje incidentov.

13. člen
(začetek veljavnosti)

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

Št. Rudi Medved l.r.

Ljubljana, dne … 2018 Minister za javno upravo

EVA 2018-3130-0031