|  |  |
| --- | --- |
| Številka:  | 386-10/2024-1544-4 |
| Datum: | 02. 02. 2024 |

|  |  |
| --- | --- |
| **Zadeva:** | **Usmeritve za doseganje skladnosti zavezancev – organov državne uprave z Zakonom o informacijski varnosti in podzakonskimi predpisi** |

Organi državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti in so bili s sklepom Vlade Republike Slovenije določeni za zavezance na podlagi Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23, v nadaljevanju: ZInfV), so dolžni izpolnjevati zahteve iz ZInfV in Uredbe o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave (Uradni list RS, št. [98/23](http://www.uradni-list.si/1/objava.jsp?sop=2023-01-2741), v nadaljevanju: Uredba). Zahteve morajo izpolniti v enem letu od določitve s sklepom Vlade Republike Slovenije.

Obveznosti organov državne uprave (v nadaljevanju: zavezanci) so določene v 16. (varnostne zahteve), 17. (varnostna dokumentacija in varnostni ukrepi) in 18. (priglasitev incidentov) členu ZInfV, podrobneje pa urejene v Uredbi. Zavezanci so dolžni vzpostaviti in vzdrževati dokumentiran sistem upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja, ki mora obsegati najmanj naslednjo dokumentacijo:

1. analizo obvladovanja tveganj z oceno sprejemljive ravni tveganj;

2. politiko neprekinjenega poslovanja z načrtom njegovega upravljanja;

3. seznam informacijskih sistemov in delov omrežja organov državne uprave ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev organov državne uprave;

4. načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov iz prejšnje točke;

5. načrt odzivanja na incidente s protokolom obveščanja CSIRT organov državne uprave in

6. načrt varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov organov državne uprave.

Na podlagi zgoraj navedene varnostne dokumentacije so zavezanci dolžni pripraviti in izvajati potrebne varnostne ukrepe, ki se delijo na organizacijske, logično-tehnične in tehnične ukrepe.

Za zagotovitev skladnosti zavezancev z ZInfV: pripravo zahtevane dokumentacije in izvedbo potrebnih varnostnih ukrepov, za obvladovanje tveganj glede varnosti za informacijske sisteme in dele omrežja, s katerimi upravljajo oziroma za informacijske storitve, ki jih izvajajo in so nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti, je potrebno zaporedno izvesti nekatere korake, ki so predstavljeni v nadaljevanju.

1. **Izvedba ocene vpliva na poslovanje (BIA analiza)**

Ocena vpliva na poslovanje (ang. Business Impact Analysis, BIA) je sicer eden ključnih in obveznih dokumentov v procesu priprave politike neprekinjenega poslovanja in načrta njenega upravljanja je pa tudi ključen dokument za pripravo seznama informacijskih sistemov in delov omrežja zavezanca ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev zavezanca. Z izvedbo ocene vpliva na poslovanje popišemo vse procese v organizaciji oziroma zavezancu, prepoznamo ključne (kritične) procese in jih z uporabo ustrezne metodologije ocenimo iz vidika zaupnosti, celovitosti ter razpoložljivosti in sicer kakšna škoda (materialna in predvsem nematerialna) bi nastala pri neželeni prekinitvi posameznega procesa.

V prvi fazi je potrebno popisati vse (delovne) procese v organizaciji oziroma zavezancu. Izmed popisanih procesov se prepozna in določi ključne procese.

Pri določanju ključnih procesov izhajamo iz področnih zakonskih nalog, ki jih je zavezanec dolžan zagotavljati oziroma izvajati ob vsakem času, te naloge pa so nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti. Od pomembnosti posameznega procesa je tudi odvisna določitev toleriranega časa nedelovanja (izpada) za posamezni proces in potreba po zagotavljanju rezervnih postopkov za nadaljevanje izvajanja procesa v primeru prekinitve oziroma izpada (kar je sicer del politike neprekinjena poslovanja, katerega sestavni del je ocena vpliva na poslovanje).

Ocena vpliva na poslovanje tako zajema navedbo možnih dogodkov in incidentov, ki vplivajo na izvajanje procesov/nalog organizacije oziroma organa oziroma imajo vpliv za zaupnost, celovitost in razpoložljivost informacij/sistemov. Najmanj je potrebno izvesti oceno vpliva na poslovanje zaradi odpovedi informacijskih sistemov, pomanjkanja zaposlenih, izpada posamezne lokacije in odpovedi storitev pogodbenih izvajalcev.

Po določitvi (ključnih) procesov organizacije oziroma organa je potrebno prepoznati lastnike teh procesov, ki so tudi pristojni za oceno vpliva na zaupnost, celovitost in razpoložljivost. Lastniki procesov tudi opravijo presojo vpliva toleriranega časa izpada posameznega procesa, kar je osnova za določitev prioritet in časovnih okvirjev za nadaljevanje procesa ter izvedbo potrebnih ukrepov.

Popis (poslovnih) procesov organa naj bi obsegal najmanj:

1. naziv procesa;

2. odgovorno osebo za proces (lastnik procesa);

3. kritičnost procesa (npr. nizka/visoka ali nizka/srednja/visoka);

4. tip procesa (glavni/podporni proces);

5. sredstva (viri) za izvajanje (podporo) procesa (informacije v elektronski/fizični obliki, zaposleni uslužbenci, pogodbeni partnerji, strojna oprema, programska oprema, komunikacijska oprema, podporna infrastruktura, prostori, podporne storitve);

6. toleriran čas izpada procesa in

7. stopnjo vpliva na celovitost, zaupnost in razpoložljivost informacij.

Izvedbo ocene vpliva na poslovanje določa in opredeljuje tudi mednarodni standard neprekinjenega poslovanja SIST ISO/IEC 22301:2019, pri izvedbi ocene vpliva na poslovanje pa je potrebno upoštevati najmanj zahteve iz 5. člena Uredbe.

1. **Določitev informacijskih sistemov in delov omrežja organov državne uprave ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev organov državne uprave**

Ustrezno izvedena ocena vpliva na poslovanje (določitev in ovrednotenje ključnih procesov) zavezanca je podlaga za pripravo seznama informacijskih sistemov in delov omrežja organa državne uprave ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev organa državne uprave. Na seznam tako sodijo vsi informacijski viri, ki neposredno (ali posredno) podpirajo oziroma omogočajo izvajanje ključnih (kritičnih) procesov, ki so bili kot taki prepoznani oziroma določeni v oceni vpliva na poslovanje.

Za vsak tak informacijski sistem (vir) je potrebno navesti upravljalca (skrbnika) sistema oziroma posameznega informacijskega vira. Upravljalci oziroma skrbniki (lastniki) posameznih informacijskih virov se navedejo z imenom in priimkom ali z delovnim mestom, kjer je nedvoumno razvidno, katera oseba je bila v določenem času skrbnik (lastnik) posameznega informacijskega vira. V kolikor je kot upravljalec oziroma skrbnik informacijskega sredstva navedena organizacijska enota zavezanca je odgovornost na vodji organizacijske enote. Pri pripravi seznama informacijskih sistemov in delov omrežja organa državne uprave ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev organa državne uprave je potrebno upoštevati 6. člen Uredbe, ki določa, da mora tak seznam, poleg informacijskih sistemov (virov), vsebovati tudi vsa druga sredstva, od katerih je odvisno zagotavljanje storitev organa državne uprave (npr. ključni zaposleni, prostori, napajanje, hlajenje, varovanje, ipd.).

1. **Izvedba analize obvladovanja tveganj in ocena sprejemljive ravni tveganj**

Tveganje je definirano kot učinek negotovosti na doseganje ciljev. Namen ocene tveganja je identifikacija groženj in podaja ocene, kako visoko tveganje grožnje predstavljajo za organizacijo/organ glede na uresničitev zahtev varovanja informacij z vidika zaupnosti, celovitosti in razpoložljivosti informacij. Tako tveganja ocenjujemo z vidika ocene posledic uresničitve grožnje in verjetnosti uresničitve grožnje.

Ustrezno določeni informacijski sistemi in deli omrežja organa državne uprave ter pripadajoči podatki, ki so bistvenega pomena za delovanje storitev organa državne uprave so podlaga za izvedbo procesa analize obvladovanja tveganj (vrednotenje sredstev po pomembnosti).

Praviloma so skrbniki posameznih procesov oziroma skrbniki (lastniki) posameznih informacijskih virov tudi skrbniki (lastniki) posameznih tveganj. Za določitev sprejemljive ravni tveganj pa je odgovorno vodstvo organa. Določitev sprejemljive ravni tveganj pomeni, da bo zavezanec za vsa prepoznana tveganja, ki so se znašla nad določeno sprejemljivo ravnjo tveganj, izvajal ukrepe za zmanjšanje teh tveganj.

Predmet analize obvladovanja tveganj so tako posamezni (ključni) informacijski viri (lahko pa so tudi posamezni procesi). Lastnik informacijskega sredstva v postopku izvajanja ocene tveganj oceni njegovo vrednost v primeru izgube zaupnosti, celovitosti in razpoložljivosti. V velikih sistemih je mogoče posamezna informacijska sredstva, na podlagi popisa sredstev, razvrstiti v posamezne kategorije sredstev (večja preglednost analize obvladovanja tveganj) in oceniti njihovo vrednost v primeru izgube zaupnosti, celovitosti in razpoložljivosti po kategorijah . Takšne kategorije informacijskih sredstev (virov) so lahko na primer: informacije v elektronski obliki (baze podatkov, datoteke, dokumenti), informacije v fizični obliki (papirni dokumenti, slikovni izpisi), strojna oprema (strežniki, mrežna oprema, delovne postaje, prenosni računalniki), programska oprema (operacijski sistemi, aplikacije, licenčna programska oprema), prenosne naprave (prenosni računalniki, tablični računalniki), nosilci podatkov, komunikacije, infrastruktura, prostori, in osebje (administratorji, lastniki informacijskih sredstev, uporabniki).

Analiza obvladovanja tveganj se izvede glede na kriterije: verjetnosti uresničitve grožnje, stopnje posledic uresničitve grožnje, stopnje ranljivosti informacijskih sredstev (virov) in učinkovitosti uporabljenih ukrepov posamezna informacijska sredstva (procese) ali posamezne kategorije informacijskih sredstev

Nominalni kriteriji (lestvica, npr. od 1 do 5) za oceno vpliva na zaupnost, celovitost in razpoložljivost se določijo glede na specifičnost področja dela organa. Najvišja ocena od enega od treh kriterijev je podlaga na nadaljnjo vrednotenje. Za vsako sredstvo oziroma določene kategorije sredstev je potrebno popisati oziroma prepoznati možne grožnje, ki lahko vplivajo nanj (izgubo zaupnosti, celovitosti, razpoložljivosti) in prepoznati ranljivosti sredstev, ki bi jih prepoznane grožnje lahko prizadele ter opredeliti verjetnost uresničitve grožnje (npr. NIZKA - grožnja se ni uresničila v zadnjih 2 letih, SREDNJA - grožnja se je uresničila v zadnjih dveh letih enkrat, VISOKA – grožnja se je uresničila v zadnjih dveh letih več kot enkrat). Na podlagi ustrezno pripravljene matrike se potem izračuna oziroma ovrednoti ugotovljena tveganja glede na verjetnost nastanka tveganj in obseg negativnih posledic ob uresničitvi tveganj na zagotavljanje storitev zavezanca in sicer glede na kriterije verjetnost grožnje, stopnja posledic uresničitve grožnje, stopnje ranljivosti sredstev ter učinkovitosti uporabljenih ukrepov.

Za ustrezno pripravo analize obvladovanja tveganj je lahko podlaga kateri od mednarodnih standardov (npr. ISO/IEC 27005:2022) ali pa Metodologija obvladovanja tveganj informacijske varnosti v državni upravi, ki jo je pripravilo Ministrstvo za javno upravo in je dostopna na spletu.[[1]](#footnote-1) Pomembno je, da so pri pripravi analize obvladovanja tveganj z oceno sprejemljive ravni tveganj upoštevane minimalne zahteve iz 4. člena Uredbe.

1. **Priprava politike neprekinjenega poslovanja in načrta njenega upravljanja**

Neprekinjeno poslovanje so aktivnosti, ki so potrebne za ohranjanje poslovanja oziroma delovanja organa/organizacije v času motenj ali prekinitev normalnega delovanja zaradi različnih vzrokov. Sistem upravljanja neprekinjenega poslovanja je sistem upravljanja, ki temelji na strateški in taktični sposobnosti organa/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 (različni scenariji).

Na podlagi popisa procesov, ki je bil obravnavan v prvem poglavju, se pripravijo oziroma navedejo postopki neprekinjenega poslovanja za tiste procese, ki so bili kot kritični (pomembni) prepoznani v oceni vpliva na poslovanje, ki je bila podrobno pojasnjena v prvem poglavju. Potrebno je navesti vse postopke in ukrepe v primeru pojava incidentov in dogodkov, ki negativno vplivajo na neprekinjeno delovanje kritičnih procesov zavezanca in določiti potrebne vire.

1. **Priprava načrta obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev, nujnih za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti**

Možnost hitrega obvladovanja incidentov lahko skrajša čas izpadov, zmanjša finančno škodo in skrajša čas izpada delovanja bistvene storitve organa. Načrt obnovitve organizacijam pomaga pri izpolnjevanju zahtev glede skladnosti s predpisi, hkrati pa zagotavljajo jasen načrt za obnovitev.

Prvi korak pri pripravi načrta obnovitve je priprava strategije obnovitve. Le-ta mora upoštevati razpoložljiva finančna sredstva, zavarovanje, vire (kadrovske, fizične zmogljivosti), stališče vodstvene ekipe o tveganjih, tehnologijo, shranjevanje podatkov, dobavitelje, zahteve glede skladnosti s predpisi.

Vodstvena odobritev strategije obnovitve je pomembna. Strategija mora biti usklajena s cilji organizacije. Ni nujno, da gre za posamezen dokument, omenjena strategija je lahko vključena v druge strateške dokumente/strategije organizacije (npr. strategija je lahko del poslovnega načrta). Ko je strategija obnovitve razvita in odobrena s strani vodstva, jo je mogoče prenesti v načrte za obnovo po nesreči.

Strategija obnovitve mora zajemati določitev časa okrevanja (ang. Recovery Time Objective, RTO) in ciljno točko obnove podatkov (ang. Recovery Point Objective, RPO). Čas okrevanja določa v kakšnem časovnem obdobju morajo aplikacije/informacijski sistemi ponovno delovati, običajno merjeno v urah, minutah ali sekundah. V oceni vpliva na poslovanje pa je treba določiti minimalni obseg storitve. Ciljna točka obnove podatkov pa opisuje starost datotek, ki jih je treba obnoviti iz pomnilnika varnostne kopije podatkov za nadaljevanje običajnih operacij.

Ko imamo opredeljene elemente obnovitvene strategije, pripravimo načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje storitev, nujnih za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti (v nadaljevanju načrt obnovitve delovanja). Gre za dokumentiran, strukturiran pristop, ki opisuje, kako lahko organizacija po nenačrtovanem incidentu hitro nadaljuje z delom. Načrt obnovitve je bistven del načrta neprekinjenega poslovanja. Cilj načrta je pomagati organizaciji razrešiti izgubo podatkov in obnoviti sistemsko funkcionalnost, tako da lahko deluje po incidentu, tudi če deluje na minimalni ravni (obseg minimalne storitve je naveden v obnovitveni strategiji).

Načrt je sestavljen iz korakov za zmanjšanje posledic nesreče, tako da lahko organizacija še naprej deluje ali hitro nadaljuje s kritičnimi funkcijami. Organizacija mora izvesti oceno vpliva na poslovanje v sklopu katerega izvede analizo poslovnih procesov (kaj potrebuješ, da bistveni procesi tečejo nemoteno), poveže s sistemom upravljanja/obvladovanja tveganj in določi cilje okrevanja (čas ponovne vzpostavitve poslovanja in točka obnavljanja podatkov – največji dopustni čas izgube podatkov pred izpadom).

Nekatere vrste nesreč, ki jih organizacije lahko načrtujejo, so napaka pri uporabi, napaka v komunikaciji, izpad električne energije, naravna nesreča, zlonamerna programska oprema ali drug kibernetski napad, katastrofa podatkovnega centra, gradbena nesreča, izliv vode, potres, požar in drugo kar organizacija oceni kot možno tveganje za njene informacijske sisteme in omrežja.

Glavni cilj načrta obnovitve delovanja je zmanjšati negativne učinke incidenta na poslovanje. Obseg načrta za obnovo po nesreči je lahko zelo osnoven, ali pa zelo celovit in lahko obsega več deset strani.

Kontrolni seznam načrta za obnovo po nesreči običajno vključuje:

* seznam oziroma popis kritičnih sistemov in omrežij organa;
* osebje, odgovorno za te sisteme in omrežja;
* opredelitev najresnejših groženj in ranljivosti;
* pregled zgodovine nenačrtovanih incidentov in izpadov ter kako so bili obravnavani;
* informacije o ciljni točki obnove podatkov in času okrevanja;
* določitev [skupine ljudi za odzivanje na incident](https://www.techtarget.com/searchsecurity/definition/incident-response-team);
* korake za ponovni zagon, ponovno konfiguracijo in obnovitev sistemov in omrežij;
* pregled in odobritev vodstva;
* testiranje načrta;
* posodobitev načrta.
1. **Priprava načrta odzivanja na incidente s protokolom obveščanja CSIRT organov državne uprave**

Načrt odzivanja na incidente je dokument, ki je del druge varnostne dokumentacije in potrjen s strani vodstva. Vsi uslužbenci, ki imajo opredeljene zadolžitve in naloge morajo biti seznanjeni z načrtom in razumeti svojo vlogo pri odzivanju na incident.

Načrt odzivanja na incidente pogosto vključuje:

* seznam vlog in odgovornosti članov skupine za odzivanje na incidente;
* povzetek orodij, tehnologij in fizičnih virov, ki morajo biti na voljo;
* seznam ključnih postopkov za obnovitev omrežja in podatkov;
* notranje in zunanje komunikacije.

Za odzivanje na incidente se lahko določi vodjo incidenta. Ta oseba vodi odziv na incident, vodi komunikacijo z deležniki in jih obvešča ter odreja vloge. Vodja incidenta praviloma ne opravlja tehničnih nalog. Po koncu incidenta pripravi analizo s predlogi za izboljšanje odzivanja. V okviru načrta se določi tehnični vodja incidenta, ki lahko vključi v odziv na incident tudi druge tehnične strokovnjake na podlagi odobritve vodstva organa in v soglasju z vodjo incidenta.

Poleg tega se določi tudi osebo za obveščanje javnosti, ki bo sodelovala z mediji in objavljala informacije na družabnih omrežjih in uradni spletni strani organa.

V okviru tega načrta se predvidi tudi osebo (lahko vodja incidenta, tehnični vodja), ki incident priglasi na SIGOV-CERT.

V okviru načrta je priporočljivo predvideti tudi usposabljanje osebja za odzivanje na incidente. Pomembno je, da le-ti razumejo pomen načrta. Ko ga ustvarite, izobražujte svoje osebje o odzivanju na incidente. Polno sodelovanje zaposlenih z IT lahko skrajša trajanje motenj. Poleg tega lahko z razumevanjem osnovnih varnostnih konceptov omejite možnosti za večjo kršitev.

1. **Priprava načrta varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov**

Zaščita podatkov organa in sistemov, ki te podatke zbirajo, obdelujejo in vzdržujejo, je ključnega pomena. Sorazmerno s tveganjem je treba izvajati ukrepe za kibernetsko varnost in zasebnost za zaščito pred nepooblaščenim dostopom, spreminjanjem, razkritjem ali uničenjem podatkov in sistemov, aplikacij in storitev. To vključuje tudi zaščito pred naključno izgubo ali uničenjem. Varnost sistemov, aplikacij in storitev mora vključevati nadzor in zaščitne ukrepe za preprečevanje morebitnih groženj ter nadzor za zagotavljanje zaupnosti, celovitosti, razpoložljivosti in varnosti.

Zaupnost se nanaša na ohranjanje pooblaščenih omejitev dostopa in razkritja pooblaščenim uporabnikom in storitvam, vključno s sredstvi za zaščito zasebnosti in lastniških informacij. Integriteta podatkov se nanaša na zaščito pred nepravilno spremembo ali uničenjem, vključno z zagotavljanjem nepreklicnosti in avtentičnosti. Dostopnost pa zadeva pravočasen in zanesljiv dostop do podatkov.

Zaščitni ukrepi se opredelijo na podlagi ocene tveganja, ki je izvedena z uveljavljeno metodologijo za ocenjevanje informacijskih varnostnih tveganj. Ukrepe za blaženje tveganj se poveže z uveljavljenimi kontrolami standardov, kot na primer NIST Cyber Security Framework[[2]](#footnote-2) ali skupina standardov ISO 27000. Skladno z preverjanjem ocene tveganj se preverja tudi načrt varnostnih ukrepov, ki se prilagaja varnostnim razmeram in spreminjajočim tveganjem

S spoštovanjem,

|  |  |
| --- | --- |
|  |  |
|  | dr. Uroš Svete |
|  | Direktor urada |

1. https://www.gov.si/assets/ministrstva/MDP/DI/Informacijska-varnost/Metodologija-obvladovanja-tveganj-informacijske-varnosti-v-drzavni-upravi.pdf [↑](#footnote-ref-1)
2. https://www.nist.gov/cyberframework [↑](#footnote-ref-2)