REPUBLIKA SLOVENIJA
URAD VLADE RS ZA INFORMACIJSKO VARNOST

Ulica gledališča BTC 2, 1000 Ljubljana

T: 01 478 4778
E: gp.uiv@gov.si
W: http://www.uiv.gov.si
Twitter: @URSIV_Slovenia

Številka: 007-19/2023-1544-4
Datum: 04. 03. 2024

Na podlagi četrtega odstavka 4. člena Uredbe o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov (uradni list RS, št. 118/23) izdajam

Priporočila za pripravo varnostne dokumentacije povezanih subjektov

1. Uvod

Povezani subjekti so državni organi, organi lokalnih skupnosti, javne agencije in nosilci javnih pooblastil ter drugi subjekti, ki niso organi državne uprave ali izvajalci bistvenih storitev po Zakonu o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) in se povezujejo s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom.

Za informacijsko varnost povezanega subjekta je odgovoren predstojnik organa oziroma odgovorna oseba pravne osebe, ki je tudi podpisnik varnostne dokumentacije. Odgovorna oseba povezanega subjekta mora določiti kontaktno osebo za informacijsko varnost in njenega namestnika ter njune podatke v 15 delovnih dneh sporočiti Uradu Vlade Republike Slovenije za informacijsko varnost. Za izvajanje nekaterih posameznih ključnih nalog na področju informacijske varnosti povezanega subjekta lahko odgovorna oseba povezanega subjekta določi tudi drugo fizično ali pravno osebo (zunanji pogodbeni ponudnik storitev).

Povezani subjekt je na podlagi prvega odstavka 18.a člena Zakona o informacijski varnosti dolžan:

1. izvesti analizo obvladovanja tveganj informacijske varnosti z oceno sprejemljive ravni tveganj;
2. sprejeti in izvajati minimalni obseg varnostnih ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov, ki upoštevajo posebne potrebe delovnega področja povezanega subjekta in
3. pripraviti navodila in postopke za obvladovanje incidentov informacijske varnosti s protokolom obveščanja CSIRT organov državne uprave (SIGOV-CERT, cert@gov.si), ki mu priglašajo incidente z možnim vplivom na centralno državno informacijsko-komunikacijsko omrežje oziroma sistem.

Pri pripravi zgoraj navedene dokumentacije mora povezani subjekt upoštevati določbe Uredbe o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov (Uradni list RS, št. 118/2023 z dne 24. 11. 2023, v nadaljevanju: Uredba), ki določa vsebino in strukturo predpisane

dokumentacije povezanih subjektov, metodologijo za pripravo analize obvladovanja tveganj informacijske varnosti z oceno sprejemljive ravni tveganj, način izvajanja obveznosti povezanega subjekta na področju informacijske varnosti, minimalni obseg varnostnih ukrepov glede informacijske varnosti ter pripravo navodil in postopkov za obvladovanje incidentov informacijske varnosti s protokolom obveščanja CSIRT organov državne uprave.

V skladu z določbami Zakona o informacijski varnosti lahko povezani subjekt nastopa v različnih situacijah oziroma vlogah, od česar so odvisne tudi njegove zakonske obveznosti in način priprave zahtevane dokumentacije. Kot centraliziran subjekt, v skladu s prvim odstavkom 74.a člena Zakon o državni upravi (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14, 51/16, 36/21, 82/21, 189/21, 153/22 in 18/23), se za namen tega navodila šteje tisti organ, čigar vse informacijsko komunikacijske sisteme upravlja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov (trenutno je to Ministrstvo za digitalno preobrazbo). Priporočila upoštevajo različne stopnje centralizacije. Tako lahko organ opravlja svoje naloge ~~nastopi~~ kot povezan subjekt, ki je v celoti centraliziran ali povezani subjekt, ki ni centraliziran ali je delno centraliziran (upravlja tudi svoje informacijske komunikacijske sisteme).

V primeru, da v fazi priprave varnostne dokumentacije ugotovite, da kot povezani subjekt sami upravljate z informacijskimi sistemi in deli omrežja oziroma izvajate informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti, o ugotovljenem stanju obvestite pristojni nacionalni organ za informacijsko varnost (Urad Vlade RS za informacijsko varnost, gp.uiv@gov.si), ki vam bo posredoval ustrezno usmeritev za nadaljnje delo.

2. Analiza obvladovanja tveganj

Tveganje je definirano kot učinek negotovosti na doseganje ciljev. Namen ocene tveganja je identifikacija groženj in podaja ocene, kako visoko tveganje posamezne grožnje predstavljajo za povezan subjekt z vidika zaupnosti, celovitosti in razpoložljivosti informacij povezanega subjekta ter posledično nastanka posledic na delovanje državnega informacijsko-komunikacijskega omrežja oziroma sistema v primeru uresničitve grožnje. Tako tveganja ocenjujemo z vidika verjetnosti uresničitve grožnje in ocene posledic uresničitve grožnje.

Ustrezno popisani informacijski sistemi in deli omrežja, iz katerega se povezani subjekt povezuje v centralno državno informacijsko-komunikacijsko omrežje so podlaga za izvedbo procesa analize obvladovanja tveganj. V popis informacijskih sredstev znotraj sistema upravljanja varovanja informacij oziroma omrežja sodi tudi določitev upravljavcev za tiste sisteme, ki jih povezan subjekt upravlja sam.

Praviloma so skrbniki (lastniki) posameznih informacijskih virov/sredstev tudi skrbniki (lastniki) posameznih tveganj. Za določitev sprejemljive ravni tveganj pa je odgovorno vodstvo povezanega subjekta. Določitev sprejemljive ravni tveganj pomeni, da bo povezan subjekt za vsa prepoznana tveganja, ki so se znašla nad določeno sprejemljivo ravnjo tveganj, izvajal ukrepe za zmanjšanje le-teh ~~tveganj~~.

Povezani subjekt izvede popis informacijskih sredstev znotraj sistema upravljanja varovanja informacij oziroma omrežja, iz katerega se povezuje v centralno državno informacijsko-komunikacijsko omrežje oziroma sistem ter določi njihove upravljavce. Centralizirani organi izvedejo popis informacijskih sredstev v sodelovanju z ministrstvom, pristojnim za upravljanje

informacijsko-komunikacijskih sistemov, ki jim mora na zahtevo poslati potrebne podatke. Vsako popisano informacijsko sredstvo mora imeti vsaj naslednje podatke:

1. kratko identifikacijsko oznako, s katero se to informacijsko sredstvo edinstveno identificira;
2. naziv oziroma ime informacijskega sredstva;
3. opis glavnih funkcionalnosti informacijskega sredstva;
4. opis glavnih komponent strojne oziroma programske opreme in
5. ime in priimek ali naziv delovnega mesta osebe, ki je skrbnik informacijskega sredstva.

Izvedba analize obvladovanja tveganj se prične z določitvijo oziroma opredelitvijo metodologije in lestvic ter atributov ocenjevanja, po kateri bo izvedena analiza obvladovanja tveganj v skladu z določbami 6. člena Uredbe. Za izvedbo ocene tveganj potrebuje povezani subjekt najmanj tri lestvice z določitvijo primernih vrednosti:

1. lestvica stopenj tveganja z navedbo stopenj tveganj (npr. nizko, srednje, visoko) in ustreznimi nominalnimi vrednostmi (npr. od 1 do 25) na podlagi katere bo ovrednotil rezultat;
2. lestvica vpliva na delovanje državnega informacijsko-komunikacijskega omrežja oziroma sistema v primeru uresničitve grožnje z navedbo vpliva (npr. zanemarljiv vpliv, manjši vpliv na delovanje, velik vpliv na delovanje) in nominalno oceno vpliva (npr. od 1 do 5) in
3. lestvica stopnje verjetnosti nastanka neželenih posledic z navedbo pogostosti pojava neželenega dogodka (npr. enkrat na tri leta, enkrat na tri leta ampak ne pogosteje kot dvakrat letno, dvakrat letno ampak ne pogosteje kot enkrat na mesec, več kot enkrat na mesec ampak ne pogosteje kot enkrat tedensko, pogosteje kot enkrat na teden) in stopnjo verjetnosti (npr. redko, malo verjetno, verjetno, zelo verjetno, verjetno) ter nominalno oceno (npr. od 1 do 5).

Predmet analize obvladovanja tveganj so tako posamezni informacijski viri/sredstva. Lastnik/skrbnik informacijskega sredstva v postopku izvajanja ocene tveganj najprej 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: baze podatkov, datoteke, dokumenti, strežniki, mrežna oprema (usmerjevalniki, stikala, ipd.), delovne postaje, prenosni računalniki, operacijski sistemi, aplikacije, licenčna programska oprema, prenosni računalniki, nosilci podatkov, komunikacije, infrastruktura, prostori ali osebje.

Analiza obvladovanja tveganj se izvede glede na kriterije: verjetnosti uresničitve grožnje, stopnje posledic uresničitve grožnje, stopnje ranljivosti informacijskih sredstev (virov) in učinkovitosti uporabljenih ukrepov na posamezna informacijska sredstva (procese) ali posamezne kategorije informacijskih sredstev ter učinkovitosti uporabljenih ukrepov na delovanje državnega informacijsko-komunikacijskega omrežja oziroma sistema.

Na podlagi ustrezno pripravljene matrike se nato izračuna (npr. z množenjem) 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 tudi 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] Pomembno je, da so pri pripravi analize obvladovanja tveganj z oceno sprejemljive ravni tveganj upoštevane minimalne zahteve iz 6. člena Uredbe, kjer je predpisan okvir metodologije za pripravo analize obvladovanje tveganj informacijske varnosti.

3. Navodila in postopki za obvladovanje incidentov informacijske varnosti

Povezan subjekt je dolžan izdelati in vzdrževati dokument v katerem so navodila in postopki za obvladovanje incidentov informacijske varnosti in protokol obveščanja CSIRT organov državne uprave. Povezani subjekt je dolžan obvestiti CSIRT organov državne uprave (priglasitev incidenta) o vsakem zaznanem incidentu, ki ima možen pomemben vpliv na centralno državno informacijsko-komunikacijsko omrežje oziroma sistem. Povezani subjekt pa lahko določi izvajanje prostovoljne priglasitve incidentov informacijske varnosti, ki imajo ali bi lahko imeli vpliv na njihove informacijske sisteme, a nimajo vpliva na centralni državno in informacijsko-komunikacijsko omrežje ozirom sistem.

V navedeni dokumentaciji povezan subjekt:

1. navede oziroma opiše sistem (organizacijske ukrepe in tehnološke rešitve) in predvidene postopke za zaznavo incidentov informacijske varnosti v informacijskem sistemu in delovnem okolju;
2. opiše sistem in predvidene postopke za zbiranje in zavarovanje dokazov o incidentu informacijske varnosti, vključno z dnevniškimi zapisi in revizijskimi sledmi, če te obstajajo;
3. opiše predvidene postopke za odziv, obravnavo in analizo incidentov informacijske varnosti (npr. način prijave, vključene osebe, uporaba informacijskih sredstev, ipd.), vključno z evidentiranjem vseh odzivnih aktivnosti (način dokumentiranja, obveščanje, ipd.);
4. opiše odgovornosti oseb oziroma organizacijskih enot ali pogodbenih izvajalcev (pravice in dolžnosti), ki jih je treba vključiti v odziv, obravnavo in analizo incidentov informacijske varnosti;
5. opiše postopke in odgovornosti za poročanje o incidentih znotraj in zunaj povezanega subjekta (notranja komunikacija, obveščanje javnosti, obveščanje upravljavca, obveščanje policije, ipd.) in
6. opiše protokol obveščanja o incidentu informacijske varnosti CSIRT organov državne uprave (oblika poročanja, začetno, vmesno in končno poročanje).

Obvestilo o incidentu informacijske varnosti, ki ima ali bi lahko imel pomemben vpliv na centralno državno informacijsko-komunikacijsko omrežje oziroma sistem mora vsebovati najmanj podatke, ki so določeni v tretjem odstavku 7. člena Uredbe. Pri obravnavi incidentov informacijske varnosti pa je treba upoštevati tudi Nacionalni načrt odzivanja na kibernetske incidente, ki je dostopen na spletu.[2]

[1] https://www.gov.si/assets/ministrstva/MDP/DI/Informacijska-varnost/Metodologija-obvladovanja-tveganj-informacijske-varnosti-v-drzavni-upravi.pdf.
[2] https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Dokumenti/2022-03-NOKI.pdf.

4. Sprejetje in izvajanje minimalnih varnostnih ukrepov informacijske varnosti

Povezani subjekt za zagotavljanje celovitosti, zaupnosti, razpoložljivosti omrežij in informacijskih sistemov sprejme in izvaja organizacijske, logično-tehnične in tehnične varnostne ukrepe, ki izhajajo iz analize obvladovanja tveganj informacijske varnosti in zahtev upravljavca centralnega informacijsko-komunikacijskega sistema, ki obsegajo najmanj:

1. upravljanje pooblastil za dostop (npr. postopki odobritve uporabe informacijskega sredstva uporabnikom, postopki za izvedbo takojšnje blokade pravic dostopa uporabnikov, ki so zapustili organizacijo ali zamenjali delovno mesto, izvajanje postopkov rednega pregledovanje pravic dostopa, posebni postopki za dodeljevanje in odvzem administratorskih pravic, omejenost dostopa do podatkov, sistemskih funkcij in aplikacij v skladu s politiko, ipd.);
2. varovanje dostopa do glavnih komponent strojne opreme (npr. ustrezna zaščita prostora pred nepooblaščenim dostopom, zaščita ožičenja, ipd.);
3. preverjanje identitete uporabnikov (npr. politika močnih gesel, omejitev števila neuspešnih prijav uporabnikov v omrežje, večfaktorski postopek prijave/preverjanja identitete uporabnika za oddaljene dostope, ipd.);
4. zaščita pred zlonamerno programsko kodo (npr. uporaba protivirusnih programov in njihovo redno posodabljanje, onemogočanje snemanja, nameščanja in uporabe neodobrene programske opreme, preverjanje datotek na magnetnih ali optičnih medijih in datotek, prejetih prek omrežij, preden se uporabijo glede okuženosti s škodljivo programsko opremo, varnostno preverjanje priponk elektronske pošte in snetih datotek preden se uporabijo, na poštnih strežnikih in namiznih računalnikih, ipd.);
5. zaznavanje poskusov vdorov in preprečevanje incidentov (npr. uporaba požarnih pregrad z ustreznimi nastavitvami, uporaba EDR in XDR, uporaba SIEM, postopki za pregledovanje in obravnavo alarmov v SIEM, izvajanje varnostih pregledov in vdornih testov, ipd.) in
6. upravljanje in preprečevanje izrab tehničnih ranljivosti (npr. izvajanje predpisanega/priporočenega posodabljanja programske opreme, spremljanje varnostnih obvestil in opozoril o pojavu ranljivosti ničelnega dne, izvajanja revizije tehničnih ranljivosti (skeniranje) strojne in programske opreme v informacijskem sistemu, ipd.).

Ukrepe iz 4. do 6. točke za povezane subjekte, ki so centralizirani izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov. Pri načrtovanju in izvajanju varnostnih ukrepov povezani subjekti upoštevajo tudi mednarodne standarde (ISO/IEC 27001, NIST, ipd.) in dobre prakse na področju informacijske varnosti. Povezani subjekti upoštevajo tudi posebne potrebe delovnega področja povezanega subjekta ter varnostne zahteve upravljavca centralnega informacijsko-komunikacijskega sistema, ki jih ta objavi na svoji spletni strani.

Varnostni ukrepi morajo biti:

- učinkoviti tako, da povečajo informacijsko varnost glede na obstoječe in predvidene grožnje, ki izhajajo iz analize obvladovanja tveganj z oceno sprejemljive ravni tveganj;
- prilagojeni tako, da se prizadevanja povezanega subjekta usmerijo v ukrepe, ki najbolj vplivajo na njegovo informacijsko varnost, povezano s centralnim državnim informacijsko-komunikacijskim omrežjem oziroma sistemom, in se izogibajo podvajanjem;
- skladni tako, da se primarno obravnavajo osnovne in skupne varnostne ranljivosti povezanega subjekta, ki se lahko dopolnijo z varnostnimi ukrepi za posamezna področja;

- sorazmerni s tveganji tako, da se izogiba čezmerni obremenitvi povezanega subjekta; konkretni tako, da povezani subjekt te varnostne ukrepe izvaja in da ti ukrepi prispevajo h krepitvi njegove informacijske varnosti in
- preverljivi tako, da povezani subjekt lahko na zahtevo pristojnega organa predloži dokazila o njihovem izvajanju in vključujoči tako, da so upoštevani vsi vidiki informacijske varnosti, vključno s fizično varnostjo informacijskih sredstev.

Uredba določa, da za povezane subjekte, ki so centralizirani, zaščito pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov ter upravljanje in preprečevanje izrab tehničnih ranljivosti izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov. Vso ostalo dokumentacijo (in izvajanje varnostnih ukrepov) so povezani subjekti dolžni izvajati v skladu z Uredbo. Povezan subjekt, ki ni centraliziran, mora pripraviti zahtevano dokumentacijo iz Uredbe v celoti. Povezan subjekt, ki je delno centraliziran mora pripraviti za necentraliziran del dokumentacijo v celoti, za centraliziran del pa upoštevati, da zaščito pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov ter upravljanje in preprečevanje izrab tehničnih ranljivosti izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov.

dr. Uroš Svete
Direktor urada