REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Napotki za priglašanje incidentov

Junij 2026

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
X: @URSIV_Slovenia

Številka: 800-6/2025-1544-5
Datum: 03. 06. 2026

Zadeva: NAPOTKI ZA PRIGLAŠANJE INCIDENTOV

Incident je dogodek, ki je ogrozil zaupnost, celovitost, razpoložljivost ali avtentičnost shranjenih, prenesenih, ali obdelanih podatkov ali storitev, ki jih omrežni in informacijski sistemi zagotavljajo, ali so prek njih dostopni. V tem kontekstu ne gre za incidente v kibernetskem prostoru temveč tudi za širši vidik incidentov informacijske varnosti. Torej je treba priglašati in poročati tudi o pomembnih incidentih, katerih vzrok je človeška namerna ali nenamerna napaka, kot na primer napake pri nadgradnjah programske opreme, pretrganje električnih ali drugih kablov, požar in drugo. Incident pomeni uresničeno grožnjo (požar, pretrganje kablov, napake pri posodobitvi programske opreme in drugo) napram informacijskim sistemom in omrežjem.

V primeru, da se je incident zgodil zaradi izkoriščene ranljivosti, se uporabljajo enaki postopki kot za priglasitev incidenta.

V primeru, da se odkrije ranljivost[1] informacijskega sistema ali omrežja, se le-to priglasi na SI-CERT, saj je SI-CERT skladno z 17. in 59. členom ZInfV-1 v Republiki Sloveniji določen kot koordinator usklajenega razkrivanja ranljivosti in vsebino obravnava v okviru Politike usklajenega razkrivanja ranljivosti (ang. Coordinated Vulnerability Disclosure, CVD).

1. Korak: Ugotovitev ali se je zgodil incident

Pri ugotavljanju, ali gre za incident je treba preveriti, ali se je zgodil dogodek, ki je ogrozil zaupnost, celovitost, razpoložljivost ali avtentičnost shranjenih, prenesenih, ali obdelanih podatkov ali storitev, ki jih omrežni in informacijski sistemi zagotavljajo, ali so prek njih dostopni. Omenjen dogodek se lahko zgodi v kibernetskem prostoru ali izven njega. Torej je povzročitelj dogodka lahko zlonamerni kibernetski akter, ki na primer uporabi zlonamerno programsko opremo, pošilja elektronska sporočila spletnega ribarjenja, ali pa je dogodek posledica nekibernetskih dejavnikov kot so požar, poplave, pretrganje kablov in podobno.

V nadaljevanju so predstavljene definicije po družini standardov ISO/IEC 27000 in primeri kršenja, oziroma ogrožanja zaupnosti, celovitosti, razpoložljivosti ali avtentičnost, shranjenih, prenesenih, ali obdelanih podatkov ali storitev. Za lažje razumevanje so opisani tudi primeri.

Zaupnost (Z) je opredeljena kot lastnost, da informacije niso dostopne ali razkrite nepooblaščenim posameznikom, entitetam ali procesom. Incident kršitve zaupnosti je dogodek, pri katerem pride do nepooblaščenega razkritja informacij, nepooblaščenega dostopa do informacij, uhajanja podatkov, vpogleda oseb brez ustreznih pravic. Primer kršenja zaupnosti je v kolikor se ne prepreči

[1] Ranljivost je pomanjkljivost, dovzetnost ali napaka proizvoda ali storitve IKT, ki jo kibernetska grožnja lahko izkoristi.

nepooblaščen dostop do podatkov, kar bi se lahko zgodilo z vdorom do baze podatkov strank določenega subjekta. V tovrstnih primerih zlonamerni akterji tako pridobljene podatke bodisi zaklenejo z izsiljevalsko programsko opremo in nato zahtevajo odkupnino bodisi grozijo ali že celo objavijo pridobljene podatke na temnem spletu.

Celovitost (C) je opredeljena kot lastnost točnosti in popolnosti informacij ali podatkov. Incident kršitve celovitosti pomeni nepooblaščeno spremembo podatkov, poškodovanje podatkov, manipulacijo vsebine, izgubo točnosti ali popolnosti informacij. Celovitost je kršena, ko ni mogoče potrditi, da so podatki točni, popolni in da niso bili nepooblaščeno spremenjeni. To bi se lahko zgodilo v primeru nepooblaščenega spreminjanja podatkov. V primeru spletne banke bi zlonamerni kibernetski akterji prestregli transakcijo in spremenil številko TRR prejemnika ali znesek nakazila, preden sistem obdela zahtevo. Podatki so bili spremenjeni med procesom, kar pomeni, da informacija v sistemu ni več verodostojna.

Razpoložljivost (R) je opredeljena kot lastnost pri kateri so informacije dostopne in uporabne na zahtevo pooblaščenega subjekta. Incident kršitve razpoložljivosti je dogodek pri katerem je prišlo do nedosegljivosti sistema ali podatkov, prekinitve storitve, izgube dostopa. Razpoložljivost je kršena, ko sistemi, podatki ali storitve niso dostopni uporabnikom, ko jih ti potrebujejo, kot je na primer pri brisanju oziroma popolni odstranitvi podatkov iz naprave, sistema ali nosilca podatkov (ang. Wiping), ali pri onemogočanju delovanja storitev (npr. DDoS napad). Zlonamerni kibernetski akterji v prvem primeru trajno odstranijo, ali prepišejo podatke in jih zato ni mogoče enostavno obnoviti. Pri DDoS napadu pa s pomočjo tisoč okuženih računalnikov preplavijo spletno stran z zahtevki, ki jih strežnik ne more obdelati, zato spletna stran postane neodzivna, legitimni uporabniki pa ne morejo dostopati do storitev ali informacij, ki delujejo na dotični spletni strani.

Avtentičnost (A) je opredeljena kot lastnost, da je entiteta to, za kar se predstavlja. Incident kršitve avtentičnosti pomeni lažno predstavljanje, krajo identitete, ponarejanje izvora informacij, uporabo lažnih poverilnic. Avtentičnost je tako ogrožena, ko se ne more potrditi identitete uporabnika ali vira podatkov. Primeri njene kršitve je na primer, ko zlonamerni akter pošlje elektronsko sporočilo, ki je videti, kot da jo je poslala banka, pri kateri je posameznik komitent ali notranji IT oddelek. Elektronska pošta vsebuje povezavo, ki osebo preusmeri na ponarejeno spletno stran, kjer oseba vpiše svoje geslo. Ker je videti pristno, gre za kršitev avtentičnosti vira.

Ko se ugotovi, da gre za incident informacijske varnosti le-tega priglasi pristojni **skupini CSIRT**, ki se odziva na incidente na področju računalniške varnosti, sprejema prijave o kršitvah varnosti, izvaja analize in pomaga priglasiteljem pri obvladovanju incidentov. Trenutno sta v Republiki Sloveniji organizirani dve skupini CSIRT in sicer SIGOV-CERT in SI-CERT. V kolikor ima subjekt z ugotavljanjem stanja glede incidenta izzive, lahko za pomoč ali mnenje zaprosi pristojno skupino CSIRT.

2. Korak: Ocena vpliva in resnost incidenta

Če se ugotovi, da je šlo za kršitev zaupnosti, celovitosti, razpoložljivosti ali avtentičnost in zato gre za incident informacijske varnosti, nastopi drugi korak v okviru katerega se oceni vpliv incidenta. Na podlagi vpliva pa se nato oceni resnost incidenta v skladu s postavljeno lestvico v okviru organizacije (podrobneje opredeljeno v nadaljevanju).
Od omenjene ocene incidenta so odvisne nadaljnje aktivnosti in zakonske obveznosti ter postopki, ki jih mora subjekt izvesti. Subjektom je zato v pomoč spodnja opredelitev pomembnega incidenta in razvrstitev incidentov glede na vpliv na ostale informacijske sisteme, storitve subjekta, druge subjekte in finančne posledice.

Pomemben incident je tisti incident, ki je subjektu povzročil ali bi mu lahko povzročil resne operativne motnje pri opravljanju storitev ali finančne izgube oziroma bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode. Pri tem se upošteva tudi prizadetost omrežnih in informacijskih sistemov, zlasti njihov pomen pri zagotavljanju njegovih storitev, resnost in tehnične značilnosti kibernetske grožnje in njenega vpliva na uporabnike, ranljivosti, ki se izkoriščajo in izkušnje s podobnimi incidenti.

Prizadeti subjekt se pri presojanju opre na lastno varnostno dokumentacijo, del katere bi moral biti tudi načrt odzivanja na incidente. V njem bi moralo biti opredeljeno, v katerih primerih bi bil incident za subjekt, glede na zgoraj opredeljeno definicijo, pomemben[2]. V nadaljevanju je naveden primer kot pomoč za razvrščanje in ocenjevanje dogodkov.

Incidenti se lahko razvrstijo v štiri kategorije oziroma stopnje glede na resnost incidenta in sicer: S1 (kritično), S2 (visoko), S3 (srednje) in S4 (nizko). Na podlagi razvrstitve se določijo in izvedejo nadaljnji ukrepi, obveščanja in poročanja.

Kadar je razvrščanje oziroma vrednotenje pomembnosti incidenta na mejnih vrednostih meril, se za vrednotenje upošteva višja stopnja.

V primeru, da organizacija incident ovrednoti s stopnjo najmanj S2 gre za pomemben incident, in ga je dolžna v skladu z ZInfV-1 priglasiti pristojni skupini CSIRT.

Tabela 1: Razvrščanje glede na resnost in odzivni časi

Stopnja	Opis/merila	Primeri/posledice	Začetni odzivni čas
S1 Kritično	Velik neposreden negativni vpliv na delovanje kritičnih storitev; velika verjetnost velike poslovne škode, ki lahko ogrozi preživetje organizacije; veliko tveganje za upad ugleda organizacije; velik čezmejni vpliv	Izsiljevalska programska koda na ključnih sistemih z izpadom storitev; kompromitacija priviligiranega AD/IdP; kompromitacija osebnih podatkov velikega obsega ali poslovnih skrivnosti; delna ali popolna degradacija storitev	15 min
S2 Visoko	Motnje ali pomembna degradacija storitev; možno širjenje; nastanek večje poslovne škode s še obvladljivimi posledicami za poslovanje organizacije; odtujeni pomembni podatki	Privilegiran dostop napadalca; aktivna eksfiltracija podatkov; DDoS napad na ključno aplikacijo s pomembno degradacijo storitev; kritična ranljivost na sistemu z znaki izrabe; motnje v delovanju storitev	30 min
S3 Srednje	Omejen vpliv, nadzorovano širjenje, poslovna škoda je kratkoročna in sprejemljiva	Posamezna okužba končne točke brez vpliva na storitev; posamezen kompromitiran račun brez eksfiltracije; uspešen phishing posameznika brez posledic; napaka konfiguracije z nizkim tveganjem; minimalne motnje v delovanju storitev	štiri ure
S4 Nizko	Dogodki z minimalnim tveganjem, ki nimajo pomembnega vpliva na poslovanje organizacije	Lažno pozitivno SIEM opozorilo; poskusi napada brez uspeha; pravočasno izvedene aktivnosti za zamejevanje; brez motenj v delovanju storitev	en delovni dan

[2] Kot pomoč pri preverjanju, oziroma pripravi ustreznosti varnostne dokumentacije, si lahko subjekti pomagajo z Vzorčno varnostno dokumentacijo, ki jo je pripravil Urad Vlade Republike Slovenije za informacijsko varnost.

Subjekti po lastni presoji glede na zgoraj izpostavljene elemente ovrednoti stopnjo incidenta. Le-to dokončno potrdi ali spremeni pristojna skupina CSIRT skladno s 36. členu ZInfV-1. V primeru, da se ob poročanju na pristojnem nacionalnem organu ugotovijo nove informacije, lahko tudi slednji prevrednoti stopnjo incidenta.

Opomba: Ponudniki storitev DNS, registri TLD imen, ponudniki storitev računalništva v oblaku, ponudniki storitev podatkovnih centrov, ponudniki omrežij za dostavo vsebine, ponudniki upravljanih storitev, ponudniki upravljanih varnostnih storitev in ponudniki spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja pri vrednotenju ali gre za pomembni incident ter pri priglašanju incidentov upoštevajo določila Izvedbene uredbe Evropske komisije o določitvi pravil za uporabo Direktive 2022/2555/EU v zvezi s tehničnimi in metodološkimi zahtevami ukrepov za obvladovanje tveganj za kibernetsko varnost ter podrobnejšo opredelitvijo primerov v katerih se incident šteje za pomembnega.

3. Korak: Priglasitev pomembnih incidentov

- Kdo priglasi?

Bistveni in pomembni subjekti po ZInfV-1 so obvezani priglasiti pomembne incidente v zakonsko določenem roku.

Zavezanci lahko vse ostale incidente, kibernetske grožnje in skorajšnje incidente ter ranljivosti priglasijo prostovoljno na pristojno skupino CSIRT.

Subjekti, ki niso zavezanci po ZInfV-1 lahko vse incidente, kibernetske grožnje in skorajšnje incidente ter ranljivosti priglasijo prostovoljno na SI-CERT.

- Kdaj priglasi?

Zgodnje sporočilo o pomembnem incidentu morajo bistveni in pomembni subjekti poslati nemudoma, oziroma najpozneje v 24 urah po zaznavi. V zgodnjem sporočilu priglasitelj navede vse v tistem trenutku znane informacije, iz katerih je po potrebi razvidno ali je bil incident povzročen z nezakonitim in zlonamernim dejanjem in ali bi lahko imel čezmejni vpliv.

Priglasitev incidenta subjekt opravi najkasneje v 72 urah po zaznavi, ko se po potrebi dopolnijo, oziroma posodobijo že posredovane informacije, navede začetna ocena, resnost in vpliv ter podatki o kazalnikih ogroženosti, če so ti na voljo. Pristojna skupina CSIRT lahko zahteva od priglasitelja poročilo o napredku, oziroma posodobitvah stanja in izvedenih aktivnostih. Poleg tega je priporočljivo, da priglasitelj navede vse relevantne informacije vezane na incident, vključno z morebitnim medsektorskim vplivom incidenta.
V primeru, da pomemben incident poteka več kot en mesec, zavezanec predloži poročilo o napredku, končno poročilo pa najpozneje en mesec po rešitvi incidenta. Končno poročilo mora vsebovati poleg opisa, ocene resnosti in vpliva incidenta, vrste grožnje in temeljnega vzroka, izvedene blažilne ukrepe ter po potrebi čezmejni vpliv.

- Komu priglasi?

Priglasitev pomembnih incidentov in vsa nadaljnja poročila, kot tudi prostovoljne priglasitve incidentov zavezanci in subjekti, ki niso zavezanci po ZInfV-1, posredujejo po elektronski pošti pristojni skupini CSIRT vse razpoložljive informacije o incidentu.

Na SIGOV-CERT (cert@gov.si) priglasijo incidente subjekti javne uprave na državni[3] in lokalni ravni[4] ter ponudniki storitev zaupanja, ki jih izvajajo subjekti državne uprave.
Na SI-CERT (cer@cert.si) priglasijo incidente zavezanci, ki niso v pristojnosti SIGOV-CERT in subjekti, ki niso zavezanci po ZInfV-1, njihova priglasitev pa se obravnava kot prostovoljna.

Organi državne uprave, ki imajo organizirane varnostno-operativne centre v skladu z drugim odstavkom 39. člena ZInfV-1 kot tudi drugi bistveni in pomembni subjekti z omenjeno zmogljivostjo, morajo zagotoviti, da varnostno-operativni centri pomembne incidente priglasijo pristojni skupini CSIRT.

- Kaj priglasi?

Priglasitelj pristojni skupini CSIRT v elektronskem sporočilu posreduje informacijo o vrsti priglasitve (obvezna ali prostovoljna), podatke o prijavitelju oziroma organizaciji (naziv, davčna ali matična številka, sektor, podatke o kontaktni osebi in njeni dosegljivosti) in podatke o incidentu (datum in čas začetka in odkritja, opis z razpoložljivimi tehničnimi informacijami, vzrokom incidenta, prizadetimi storitvami in izvedenimi ukrepi ter oceno morebitnega medsektorskega in čezmejnega vpliva).

Poleg tega je priporočljivo, da priglasitelj navede kateri pristojni organi so bili poleg skupine CSIRT že obveščeni o incidentu (na primer Policija, Informacijski pooblaščenec).

V nadaljevanju shema ponazarja priglašanje pomembnih incidentov po 30. členu ZInfv-1 za bistvene in pomembne subjekte ter subjekte, ki niso zavezanci po ZInfV-1.

[3] Subjekti javne uprave na državni ravni so ministrstva, organi v njihovi sestavi, vladne službe in upravne enote ter tisti javni infrastrukturni zavodi, ki so ustanovljeni v skladu z zakonom, ki ureja znanstvenoraziskovalno in inovacijsko dejavnost. Mednje spadajo tudi drugi subjekti javne uprave iz Priloge 3, ki je kot Priloga sestavni del ZInfV-1.
[4] Subjekti javne uprave na lokalni ravni so občine. Konkretno gre za mestne občine kot je opredeljeno v Prilogi 2, ki je kot Priloga sestavni del ZInfV-1.

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

Priglasitev pomembnih incidentov