URSIV

KIBERNETSKO VARNI

Urad Vlade Republike Slovenije
za informacijsko varnost

Ulica gledališča BTC 2
1000 Ljubljana

gp.uiv@gov.si
01 478 47 78

SPLETNA STRAN URSIV

*Zloženka je informativne narave; zavezujoče je izključno uradno besedilo ZInfV-1 v Uradnem listu RS.

Priglasitev pomembnih incidentov

Subjekti javne uprave na državni in lokalni ravni ter ponudniki storitev zaupanja, ki jih izvajajo subjekti državne uprave.

Zavezanci, ki niso zajeti v pristojnosti SIGOV-CERT in prostovoljna priglasitev subjektov, ki niso zavezanci po ZInfV-1.

SIGOV-CERT (v okviru URSIV)

SI-CERT (v okviru ARNES)

ZGODNJE SPOROČILO
Začetna ocena incidenta in vsaj podatek o čezmejnem vplivu

PRIGLASITEV INCIDENTA
Ocena incidenta, njegova resnost in vpliv, vključno s kazalniki ogroženosti

VMESNO POROČILO O STANJU
Poda na zahtevo CSIRT

KONČNO POROČILO
EN MESEC PO PRIGLASITVI
Podroben opis incidenta z njegovim vplivom in sprejetimi ukrepi

POROČILO NAPREDKU
Incident po enem mesecu od priglasitve še vedno poteka

KONČNO POROČILO
EN MESEC PO REŠITVI INCIDENTA

Prostovoljna priglasitev

Ta možnost velja za:

- subjekte, ki niso zavezanci po zakonu,
- zavezance, kadar incident ni razvrščen kot "pomemben", a bi kljub temu lahko vplival na varnost, stabilnost ali zanesljivost informacijskih sistemov.

Prostovoljna priglasitev ni kaznovana in se ne šteje kot priznanje neskladnosti, ampak kot dejanje dobre prakse in odgovornega ravnanja.

Prostovoljna priglasitev je še posebej priporočljiva, kadar:

- Gre za nove, še neznane grožnje (npr. "zero-day" ranljivosti)
- Incident vpliva na več organizacij hkrati
- Je prizadeta informacijska infrastruktura, ki je povezana z drugimi bistvenimi storitvami
- Želi subjekt prispevati k skupni odpornosti

Kdaj je kibernetski incident pomemben?

- Kadar je zadevnemu subjektu povzročil ali bi mu lahko povzročil resne operativne motnje pri opravljanju storitev ali finančne izgube ali
- je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

Subjekti pri vrednotenju upoštevajo tudi:

- prizadetost omrežnih in informacijskih sistemov,
- resnost in tehnične značilnosti grožnje,
- ranljivosti in izkušnje subjekta s podobnimi incidenti.

PRILGASITEV INCIDENTOV

Potek inšpekcijskega nadzora

INŠPEKCIJA ZA INFORMACIJSKO VARNOST V OKVIRU URSIV

REDNO NAČRTOVANI NADZOR
V skladu s strateškimi usmeritvami in prioritetami inšpekcije

IZREDNI NADZOR
Po zaznavi odmevnega incidenta ali suma neskladnosti

- Pregled varnostne dokumentacije zavezanca (politike, postopki, načrti, ocene tveganj).
- Preverjanje izvajanja varnostnih ukrepov – ali so ukrepi le zapisani ali tudi dejansko izvajani.
- Inšpekcijski varnostni pregled omrežja – tehnični pregled za ugotavljanje ustreznosti implementacije predpisanih varnostnih kontrol in učinkovitosti zaščite.
- Ogled prostorov – fizično-tehnično varovanje lokacij, kjer se nahajajo ključni informacijski sistemi (npr. strežniške sobe).
- Ocena odzivnosti na incidente, vključno s preverjanjem ali je odzivanje ustrezno in so obveščene skupine CSIRT ter ostali deležniki.

ZAPISNIK

ODLOČBA
o odpravi ugotovljenih nepravilnosti

PREKRŠKOVNI POSTOPEK + GLOBA
V primeru ugotovljenih hujših ali večkratnih kršitev zakonskih zahtev

V primeru ugotovljenih hujših in ponavljajočih se kršitev lahko inšpektor odredi tudi izvedbo revizije skladnosti s predpisi s področja informacijske in kibernetske varnosti, ki jo izvede revizor informacijskih sistemov in tudi zavezancu odredi, da javno objavi kršitve ZInfV-1.

Pogoste ugotovitve inšpekcijskega nadzora

- Manjkajoča, nepopolna ali neustrezna varnostna dokumentacija → Ne izvaja se usposabljanj zaposlenih in ključnega IT kadra
- Varnostne zahteve do ključnih dobaviteljev niso prenesene v pogodbe, nadzor nad ključnimi dobavitelji pa se ne izvaja → Varnostne politike so "kopirane" ali generične, brez povezave z realnim stanjem organizacije ali se v praksi ne izvajajo
- Pogosto ukrepi obstajajo le "na papirju", kar pomeni, da varnostni mehanizmi niso tehnično ali organizacijsko podprti v praksi → Ni določene minimalne ravni poslovanja in postopkov za obnovo po katastrofi
- → Neizvedena ali neustrezno izvedena analiza tveganj

Inšpekcija spodbuja preventivni pristop – bolje pripravljena organizacija pomeni manj težav ob nadzoru in višjo raven zaščite pred kibernetskimi grožnjami.

Status zavezanca sam po sebi ne pomeni skladnosti z zakonom – organizacija mora sprejete ukrepe tudi dejansko izvajati in jih preverjati.

Nasvet 1: Poskrbite, da so vsi vaši dokumenti usklajeni z zahtevami ZInfV-1 in da so ukrepi kibernetske varnosti dokumentirani, uvedeni in preverljivi v praksi.

Nasvet 2: S ključnimi dobavitelji oziroma pogodbenimi partnerji sklenite anekse k veljavnim pogodbam, v katerih boste od njih zahtevali izvajanje predpisanih varnostnih ukrepov in omogočili izvajanje dolžnega nadzorstva.

INŠPEKCIJSKI NADZOR

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

Zakon o informacijski varnosti (ZInfV-1)

- ✓ **Sistemski zakon na področju informacijske in kibernetske varnosti**
- ✓ **Usklajen z EU direktivo NIS2**
- ✓ **Temelj za varnejše informacijsko okolje v javnem in zasebnem sektorju**

Urad Vlade RS za informacijsko varnost (URSIV)

Pristojni nacionalni organ za informacijsko varnost

Enotna kontaktna točka za mednarodno sodelovanje

Organ za obvladovanje kibernetskih incidentov velikih razsežnosti in kriz

Nacionalni certifikacijski organ za kibernetsko varnost

Nacionalni koordinacijski center za kibernetsko varnost

Nacionalno kibernetsko vozlišče

Glavne naloge URSIV:

- Koordinira nacionalni sistem kibernetske varnosti.
- Nudi strokovno podporo zavezancem.
- Pripravlja analize, priporočila in skrbi za preventivo.
- Organizira usposabljanja, vaje in ozaveščanje javnosti.
- Izvaja inšpekcijske nadzore.
- Objavlja anonimizirane podatke o incidentih.
- Spodbuja raziskave, dodeljuje spodbude in štipendije.
- Sodeluje z drugimi organi doma in v tujini.
- Skrbi za krizno komuniciranje in pripravlja zakonodajo.

PRIROČNIK ZA KIBERNETSKO VARNOST

Nacionalni koordinacijski center za kibernetsko varnost (NCC-SI)

NCC-SI deluje v okviru URSIV in je del evropske mreže nacionalnih koordinacijskih centrov.

Temeljne dejavnosti NCC-SI:

- Vzpostavljanje sodelovanja med podjetji, raziskovalnimi ustanovami in izobraževalnim sistemom v Sloveniji, z namenom njihovega vključevanja v evropske raziskovalno-inovacijske projekte
- Ozaveščanje javnosti in strokovne skupnosti o pomenu kibernetske varnosti ter o učinkovitih pristopih k zmanjševanju tveganj
- Krepitev kadrovskega potenciala s podporo razvoju strokovnjakov na področju informacijske in kibernetske varnosti
- Spodbujanje raziskav, razvoja in inovacij na področju kibernetske varnosti ter krepitev nacionalnih zmogljivosti in odpornosti
- Informiranje o evropskih razpisih (npr. programih DIGITAL in Obzorje Evropa) in pomoč pri pripravi prijav ter povezovanju z mednarodnimi partnerji
- Promocija kibernetske varnosti kot poklicne priložnosti med različnimi ciljnimi skupinami, predvsem med mladimi

Verjamemo, da lahko z združevanjem znanja, virov in izkušenj oblikujemo varnejši digitalni prostor – tako v Sloveniji kot v širšem evropskem okolju.

PRISTOJNI NACIONALNI ORGAN

Ključne novosti za zavezance

ZInfV-1 zajema:

Visoko kritične sektorje

- ENERGIJA
- PROMET
- BANČNIŠTVO
- ZDRAVJE
- PITNA VODA
- ODPADNA VODA
- UPRAVLJANJE STORITEV IKT
- JAVNA UPRAVA
- VESOLJE
- INFRASTRUKTURA FINANČNEGA TRGA
- DIGITALNA INFRASTRUKTURA

Druge kritične sektorje

- DIGITALNI PONUDNIKI
- RAVNANJE Z ODPADKI
- POŠTNE IN KURIRSKE STORITVE
- RAZISKAVE
- PROIZVODNJA
- MESTNE OBČINE
- PRIDELAVA, PREDELAVA IN DISTRIBUCIJA ŽIVIL
- IZDELAVA, PROIZVODNJA IN DISTRIBUCIJA KEMIKALIJ

Druge subjekte javne uprave na državni ravni

Javne agencije, javni skladi, javni zavodi in druge osebe javnega prava oziroma neodvisni državni organi

Novosti:

- Razširitev kroga zavezancev in samoregistracija
- Dodatni ukrepi za obvladovanje tveganj
- Izvajanje ocene in samoocene skladnosti
- Izvajanje rednega usposabljanja odgovornih oseb
- Vzpostavitev usklajenega razkrivanja ranljivosti
- Krepitev zaupanja v proizvode, storitve in postopke informacijsko-komunikacijske tehnologije (IKT)

Samoregistracija

Vsak zavezanec se mora samoprepoznati oziroma samoregistrirati preko mehanizma za samoregistracijo URSIV.

SAMOREGISTRACIJA

Niste prepričani, če ste zavezanec?
Postopek samoregistracije vas vodi čez določila.

Zavezanec mora ob samoregistraciji posredovati:

- ime in naslov, kontaktne podatke, matično številko ter elektronski naslov za vročanje;
- ustrezni sektor in podsektor iz Priloge 1 ali 2 ZInfV-1, v okviru katerih zavezanec izvaja storitve, ali kategorijo zavezancev, ki niso vključeni v navedeni prilogi, vendar sodijo med zavezance na podlagi tretjega odstavka 6. člena ZInfV-1;
- navedbo, ali ima subjekt vsaj 50 zaposlenih in letni promet ali bilančno vsoto najmanj 10.000.000 evrov;
- navedbo, ali ima subjekt vsaj 250 zaposlenih ali letni promet najmanj 50.000.000 evrov ali letno bilančno vsoto najmanj 43.000.000 evrov;
- kontaktno osebo za informacijsko varnost in njenega namestnika ter njune kontaktne podatke, vključno z elektronskimi naslovi in telefonskimi številkami;
- podatke o dodeljenih blokih javnih IP-naslovov;
- seznam držav članic Evropske unije, v katerih zavezanec opravlja storitve, ki sodijo na področje uporabe ZInfV-1;
- registrirane številke avtonomnih sistemov ter vsa domenska imena, ki jih zavezanec uporablja pri poslovanju.

NOVOSTI ZA ZAVEZANCE IN SAMOREGISTRACIJA

Ukrepi za obvladovanje tveganj

Zavezanci morajo sprejeti konkretne ukrepe za obvladovanje tveganj, ki grozijo njihovim informacijskim in omrežnim sistemom.

Kakšni so ukrepi za obvladovanje tveganj?
Ukrepi za obvladovanje tveganj naj bodo ob upoštevanju vseh nevarnosti učinkoviti, prilagojeni, skladni, sorazmerni, konkretni in preverljivi.

- Podpora vodstva in vključitev varnosti v poslovne načrte
- Osnovna kibernetska higiena in redna usposabljanja zaposlenih
- Preverjanje identitete uporabnikov in skrbno upravljanje dostopov
- Jasno določene odgovornosti za zaščito IT-sistemov
- Varnostne zahteve za ključne dobavitelje in ponudnike storitev
- Zagotavljanje integritete kadrov pred, med in po končanju delovnega razmerja
- Redno izvajanje varnostnih kopij
- Ohranjanje dnevniških zapisov o delovanju sistemov
- Raba kriptografije s šifriranjem, kjer je treba
- Upravljanje podatkovnega prometa in komunikacij

Ukrepi naj sledijo najboljšim evropskim in mednarodnim standardom ter upoštevajo stroške izvedbe.

POGOSTA VPRAŠANJA O ZInfV-1

Poleg tega morajo ukrepi obsegati tudi:

- Fizično in tehnično varovanje objektov in prostorov.
- Uporabo varne programske opreme.
- Upravljanje tehničnih ranljivosti.
- Zaščito pred zlonamerno programsko kodo.
- Uporabo večfaktorske avtentikacije in varne komunikacije.
- Varno upravljanje oblačnih storitev.

Sprejeti je treba ukrepe, ki so sorazmerni tveganjem, pri čemer se upošteva:

- stopnjo izpostavljenosti tveganjem,
- velikost subjekta,
- verjetnost pojava incidentov,
- resnost morebitnih incidentov, vključno z njihovim vplivom.

Vsaj enkrat letno ali v rednih obdobjih in ob zaznanih ranljivostih morajo subjekti:

- preveriti izpolnjevanje varnostnih ukrepov,
- sprejeti popravne ukrepe, če zaščita ni učinkovita.

UKREPI ZA OBVLADOVANJE TVEGANJ