Plinovodi
Povezani z energijo

OBVESTILA 13/23

Ljubljana, 13. 9. 2023

Načrt odzivanja na kibernetske incidente

NAČRT ODZIVANJA NA KIBERNETSKE INCIDENTE

IZDELAL	PREGLEDALA	ODOBRIL
Jure Šegota	Jan Šinigoj	Marjan Eberlinc
Šegota	Oton Gortnar	

1 Pravna podlaga in namen

Na podlagi določil točk Devetič in Dvanajstič Akta o ustanovitvi družbe z omejeno odgovornostjo PLINOVODI d.o.o., 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), v skladu z Nacionalnim načrtom odzivanja na kibernetske incidente, ki ga je Vlada Republike Slovenije sprejela dne 18. 3. 2021, na podlagi sklepa 40. seje Poslovodstva družbe PLINOVODI d.o.o., z dne 4. 9. 2023, sprejme Poslovodstvo družbe PLINOVODI d.o.o. Načrt odzivanja na kibernetske incidente, namen katerega je vzpostavitev enotnega vodila odzivanja na kibernetske incidente v družbi Plinovodi d.o.o. (v nadaljevanju družba ali zavezanec) ter priglasitve kibernetskih incidentov pristojnim institucijam.

2 Opredelitev ključnih izrazov

- **Incident** je vsak dogodek, ki ima dejanski negativni učinek na varnost omrežij in informacijskih sistemov.
- **Kibernetska grožnja** je možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja, sistema, storitev in podatkov.
- **Kibernetski napad** je napad prek kibernetskega prostora z namenom zlonamernega uničevanja, izpostavljanja, nadzorovanja ali spreminjanja, onemogočanja, zbiranja in oviranja katerega koli dela kibernetskega prostora.
- **Lažji incident** je enkraten incident, ki ima majhen negativni vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev. Nima večjega vpliva na nemoteno delovanje družbe in ji ni povzročil večje škode.
- **Težji incident** je enkraten incident oziroma zaporedje večjega števila različnih incidentov v kratkem obdobju, ki ima velik negativni vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev. Incident ima pomemben vpliv na nemoteno delovanje družbe in ji povzroči večjo škodo ali izgubo.
- **Kritični incident** je incident ali zaporedje incidentov, ki ima zelo velik negativni vpliv na zaupnost, celovitost in razpoložljivost omrežja, informacijskega sistema oziroma informacijskih storitev. Incident povzroči oteženo delovanje države, še posebej informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja, oziroma delno onemogoči delovanje vsaj treh področij bistvenih storitev ali enega v celoti.

3 Priglasitev incidentov

Družba Plinovodi d.o.o. skladno z določili SUVI in SUNP priglasi incident z vplivom na neprekinjeno izvajanje bistvenih storitev nacionalnemu odzivnemu centru za kibernetsko varnost CSIRT (Computer Security Incident Response Team), ki je v Sloveniji SI-CERT (Slovenian Computer Emergency Response Team).

Priglasitev vsebuje informacije, na podlagi katerih je mogoče določiti morebiten čezmejni vpliv incidenta. Pri določitvi pomembnosti vpliva incidenta se upošteva:

- število uporabnikov, ki jih je prizadela motnja pri zagotavljanju bistvene storitve,
- trajanje incidenta in
- geografska razširjenost, kar zadeva območje, na katerega incident vpliva.

Družba Plinovodi d.o.o. skladno z določili SUVI ob prijavi incidenta poskrbi za ustrezno zavarovanje dnevniških zapisov oziroma revizijskih sledi. Vse incidente se vodi v skladu s Politiko upravljanja varnostnih incidentov.

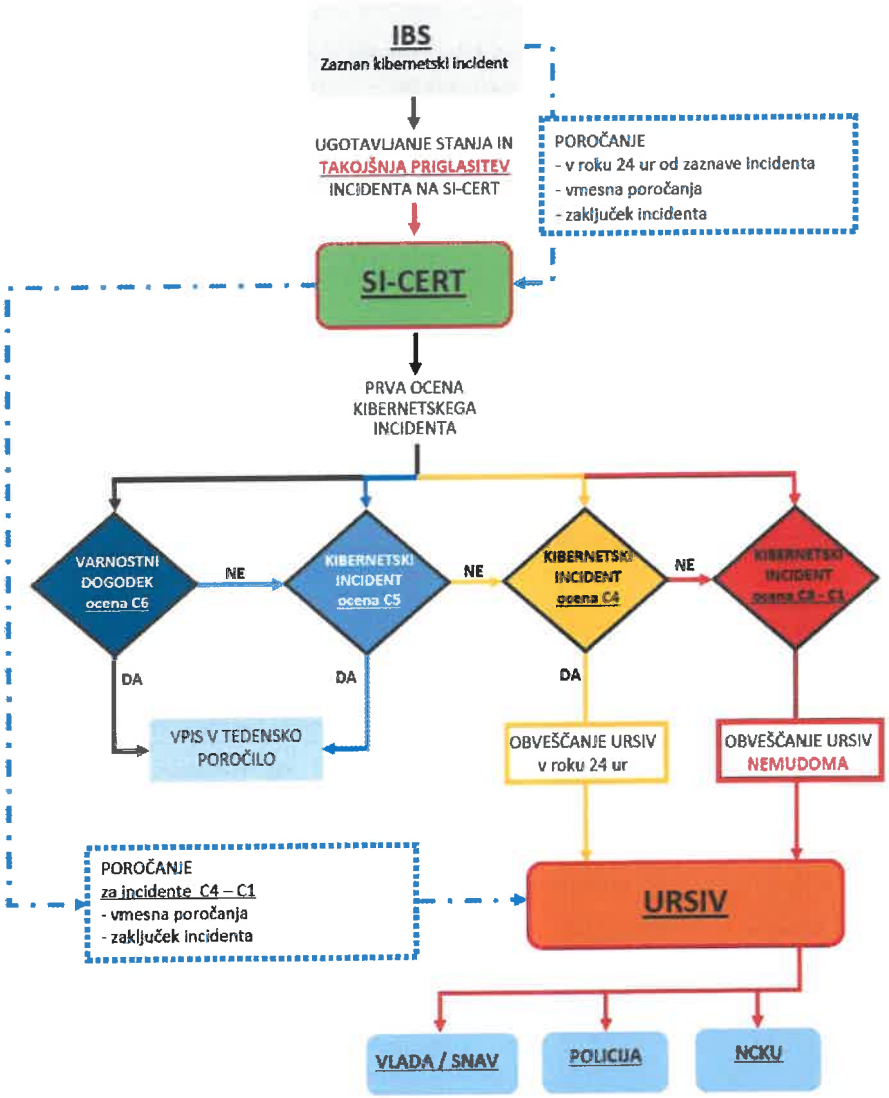
4 Klasifikacija incidentov

Skladno s Nacionalnim načrtom odzivanja na kibernetske incidente spadajo vsi incidenti, ki so povzročeni pri izvajalcu bistvenih storitev in vplivajo na neprekinjeno izvajanje bistvenih storitev, v klasifikacijo C5 in višje vse do C1. Klasifikacijo incidenta na podlagi priglašene prijave določi nacionalni CSIRT. Klasifikacija incidenta je določena na podlagi naslednje tabele:

STOPNJEVANJE V SKLADU Z ZInfV	STOPNJEVANJE NA PODLAGI KAZALNIKOV	OPIS INCIDENTA
KRITIČNI	KRITIČNI INCIDENT (C1)	– Incident povzroči oteženo delovanje države, še posebej informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja. – Povzročanje resne motnje delovanja osrednjih državnih storitev, motnja stabilnosti države. – Ima velik negativni vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev.
TEŽJI	ZELO POMEMBNI INCIDENT (C2)	– Zaznan negativni vpliv na občutljive podatke in delovanje državne in kritične infrastrukture, ki je opredeljena v 5. in 6. členu ZInfV. – Zaznan velik negativni vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. – Negativno vpliva na delovanje informacijskih sistemov obrambe, notranje varnosti ter sistema zaščite in reševanja.
	POMEMBNI INCIDENT (C3)	– Možen vpliv na izvajalce bistvenih storitev, dele državne infrastrukture in dobavno verigo za kritično infrastrukturo. – Možen negativni medpodročni vpliv.
LAŽJI	SREDNJI INCIDENT (C4)	– Zaznan majhen negativni vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. – Vpliv na izvajalce bistvenih storitev ali vpliv na gospodarstvo in dele državne uprave ali dobavno verigo.
	LAŽJI INCIDENT (C5)	– Možen vpliv na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev ali priprave na napad na gospodarstvo ali državno infrastrukturo.
KIBERNETSKA GROŽNJA	VARNOSTNI DOGODEK (C6)	– Zaznane kibernetske aktivnosti, ki nimajo vpliva na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev. – Zaznan ali možen vpliv na posamezne fizične osebe ali posamezna podjetja v državi, ki niso zavezanci.

5 Poročanje o varnostnem incidentu nacionalnemu CSIRT

Ko zavezanec priglasi kibernetski incident nacionalnemu CSIRT, se proži sistem poročanj in postopkov o kibernetskem incidentu, kot je prikazan na shemi v nadaljevanju.



Časi poročanja nacionalnemu CSIRT so odvisni od klasifikacije incidenta, kot jih v fazi prve ocene kibernetskega incidenta klasificira nacionalni CSIRT in so naslednji:

Stopnja incidenta	Začetno poročanje (od zaznave incidenta)	Vmesno poročanje (od zaznave incidenta)	Končno poročanje (po zaključenem incidentu)
C1	Nemudoma	Vsakih 6 ur	10 dni
C2		V 12 urah	5 dni
C3		V 24 urah	72 ur
C4		Po potrebi	48 ur
C5		Po potrebi	48 ur
C6	/	/	1 x tedensko

Poročanje o varnostnem incidentu s strani zavezanca poteka v treh stopnjah:

1. **začetno poročanje** (prva informacija) - poročanje o zaznavi kibernetskega incidenta v omrežju ali informacijskih sistemih in sprejetje prvih ukrepov.
2. **vmesno poročanje** - lahko jih je več, odvisno od trajanja incidenta. Poroča se o trenutnem stanju kibernetskega incidenta, s trenutnimi dostopnimi podatki in sprejetimi ukrepi, ter o poteku reševanja incidenta. Namenjeno tudi podajanju zahtevkov odzivnemu centru, URSIV ali drugim državnim službam za sodelovanje pri odpravi težav in sanaciji posledic;
3. **končno poročanje** - po zaključku incidenta se pripravi končno poročilo o poteku incidenta z vsemi podatki o incidentu, sprejetih ukrepih, posledicah, načrtu za sanacijo in odpravljanje posledic ter o ukrepih za preprečevanje ponovitve dogodka.

5.1 Vsebina poročil nacionalnemu CSIRT

Začetno poročanje (prva informacija)

Prvo informacijo o kibernetskem incidentu lahko zavezanec sporoči na kakršen koli način, ki zagotavlja hitro, zanesljivo in varno pošiljanje potrebnih informacij (telefon, e-pošta, faks, kurir ipd.). V 24 urah mora zavezanec odzivnemu centru poslati podrobno poročilo, ki mora vsebovati vse podatke iz preglednice v nadaljevanju, ki so v danem trenutku na voljo. Priporočeno je, da podatke pošlje na vzorčnem obrazcu (priloga 1). Pri izpolnjevanju poročila lahko zavezanec sodeluje z odzivnim centrom.

PRVE INFORMACIJE O KIBERNETSKEM INCIDENTU	
Podatki	Vsebina
ZADEVA	Splošni opis incidenta, s katerim bodo povezani vsi nadaljnji dokumenti v zvezi s tem incidentom.
IBS	Plinovodi d.o.o.
SEKTOR	Energetika
DATUM IN ČAS NASTANKA INCIDENTA	Čim bolj natančna časovna opredelitev nastanka incidenta.
DATUM IN ČAS ZAZNAVE INCIDENTA	Čim bolj natančna časovna opredelitev, kdaj je bil incident zaznan v sistemu.
OPIS INCIDENTA	Kratek opis zaznave in trenutnega stanja v zvezi s kibernetskim incidentom.
TAKSONOMIJA (klasifikacija) INCIDENTA	Ocenjena klasifikacija in vrsta incidenta v skladu s prilogo 2.
OGROŽENA STORITEV	Navedba, katera storitev zavezanca je ogrožena.
OCENA STOPNJE NEVARNOSTI	Primarna ocena stopnje nevarnosti, ki jo pomeni incident, in kaj je morebiti ogroženo (informacijski sistem, omrežje, informacije, storitev in drugo).
OCENA MOŽNEGA VPLIVA	Primarna ocena možnega vpliva incidenta (obseg in področje) in morebitni mednarodni vpliv.
STOPNJA INCIDENTA	Glede na merila predlagana ocena stopnje kibernetskega incidenta.

OPOMBE	Zapis vseh drugih podatkov, ki bi lahko koristili v nadaljnjem upravljanju kibernetskega incidenta.

Poleg podatkov iz predhodne tabele zavezanec sporoči odzivnemu centru tudi vse druge informacije o kibernetskem incidentu, ki jih ima v času sporočanja prve informacije na voljo in bi bile v pomoč pri upravljanju incidenta. Vsa nadaljnja komunikacija poteka glede na ocenjeno stopnjo kibernetskega incidenta in po navodilih odzivnega centra ali pristojnega nacionalnega organa. Pristojni CSIRT in pristojni nacionalni organ obravnavata incidente in podatke v skladu z ZInfV kot zaupne.

Vmesna poročila in končno poročanje

Odzivni center po prejeti prvi informaciji začne obravnavati incident in mu določi zvezno referenčno številko. Na podlagi prvega poročila opravi analizo informacij in po potrebi od zavezanca zahteva dodatne informacije. Na podlagi analize prvega poročila in z dodatnim sodelovanjem z zavezancem odzivni center določi stopnjo incidenta, ki se med upravljanjem incidenta glede na pridobljene podatke lahko spremeni.

Zavezanec glede na stopnjo incidenta in v skladu s časovnim okvirom poroča odzivnemu centru z vmesnimi poročili in ob zaključku incidenta z zaključnim poročilom o kibernetskem incidentu. Vsebina vmesnega in končnega poročila o kibernetskem incidentu je predstavljena v preglednici v nadaljevanju. Priporočeno je, da vmesno in zaključno poročilo zavezanec pošlje na obrazcu iz priloge 1.

VMESNO/KONČNO POROČILO O KIBERNETSKEM INCIDENTU	
Podatki	**Vsebina**
REFERENČNA ŠTEVILKA INCIDENTA	Referenčna številka kibernetskega incidenta, ki jo določi odzivni center in je vezana na vse dokumente o konkretnem kibernetskem incidentu.
ZADEVA	**Enaka kot v prvem poročilu** - splošni opis incidenta, s katerim bodo povezani vsi nadaljnji dokumenti v zvezi s tem incidentom.
IBS	Plinovodi d.o.o.
SEKTOR	Energetika
DATUM IN ČAS NASTANKA INCIDENTA	Čim bolj natančna časovna opredelitev nastanka incidenta.
DATUM IN ČAS ZAZNAVE INCIDENTA	Čim bolj natančna časovna opredelitev zaznave incidenta v sistemu.
OPIS INCIDENTA	Podroben opis poteka in stanja v zvezi z njim.
NAPADENA TEHNOLOŠKA SREDSTVA	Tehnični podatki o številu in vrsti sredstev, ki jih je prizadel kibernetski incident (naslovi IP, operacijski sistemi, aplikacije, strežniki in drugo).
NEDELUJOČE/ MOTENE STORITVE	Navedba, katere storitve IBS so motene ali nedelujoče, in predvideni čas do ponovne vzpostavitve teh storitev.
VZROK INCIDENTA	Vzrok kibernetskega incidenta, če je znan (odpiranje sumljive datoteke, povezovanje naprave USB, dostop do zlonamernega spletnega mesta in drugo).
TAKSONOMIJA (klasifikacija) INCIDENTA	Klasifikacija in vrsta incidenta v skladu s preglednico 1.

OCENA STOPNJE NEVARNOSTI	Ocena stopnje nevarnosti zaradi incidenta in navedba, kaj vse je lahko ogroženo (informacijski sistem, omrežje, informacije, storitev in drugo).
OCENA MOŽNEGA VPLIVA	Vpliv incidenta (obseg in področje).
STOPNJA INCIDENTA	Glede na merila ocena (za vmesno poročilo) stopnje kibernetskega incidenta.
ČEZMEJNI VPLIV INCIDENTA	Vpliv kibernetskega incidenta na katero drugo državo (katero, kakšen, kolikšen).
AKCIJSKI NAČRT IN PROTIUKREPI	Do zdaj sprejeti protiukrepi za širjenje in nadaljevanje kibernetskega incidenta ter ukrepi za odpravo kibernetskega incidenta. Nadaljnji načrtovani protiukrepi in ukrepi v zvezi s kibernetskim incidentom.
ŠKODA, POVZROČENA S KIBERNETSKIM INCIDENTOM	Ocenjena materialna škoda ali škoda, povzročena imenu zavezanca.
POTREBNO ZA ODPRAVO INCIDENTA	Tehnično osebje in tehnična sredstva, ki so potrebna za odpravo incidenta in jih zavezanec neposredno nima na voljo. Predvideno število dni za odpravo kibernetskega incidenta.
ČASOVNI OKVIR ODPRAVE POSLEDIC	Ocena, koliko časa po zaključenem incidentu bo zavezanec potreboval, da bo odpravil posledice incidenta in stanje (sistemov, omrežij, storitev in drugo) povrnil nazaj v običajno, torej kot je bilo pred kibernetskim incidentom.
PRILOGE	Seznam priloženih dokumentov, ki bodo pomagali prepoznati vzrok težave ali njeno razrešitev (posnetki zaslona, datoteke z izpisi omrežnega prometa, elektronska pošta, dnevniški izpisi in drugo).
OPOMBE	Zapis vseh drugih podatkov, ki bi lahko koristili v nadaljnjem upravljanju kibernetskega incidenta.

Zavezanec pri vmesnem poročanju izpolni polja v predhodni tabeli, za katera ima v trenutku poročanja podatke. Druge podatke pošljejo nemudoma, ko se pridobijo, če je to nujno potrebno za pravilno upravljanje incidenta ali končno poročilo.

Nacionalnemu CSIRT lahko, skladno z Zakonom o informacijski varnosti, s strani zavezanca o varnostnih incidentih poročata le Kontaktna oseba za informacijsko varnost in njen namestnik.

6 Incident v sistemih, ki obravnavajo tajne podatke

O kibernetskih incidentih in napadih na informacijske sisteme, v katerih se obravnavajo tajni podatki, je treba obvestiti organ, ki je določil tajni podatek in nacionalni varnostni organ - Urad Republike Slovenije za tajne podatke. Pri tem je treba dosledno upoštevati določila zakonodaje s področja varovanja tajnih podatkov.

Prag za obvezno poročanje zavezancev o kibernetskih incidentih v informacijskih sistemih, v katerih se obravnavajo tajni podatki in časovni okvir poročanja sta enaka kot v podpoglavju 5. Poročanje je obvezno za vse incidente, označene s stopnjo C5 in višje.

Poleg sestavnih delov prvega poročila o kibernetskem incidentu je potrebno ob prijavi dodatno posredovati še:

- podatke, potrebne za opredelitev tajnega podatka (opis medija, ki vsebuje tajni podatek, vključno s stopnjo tajnosti podatka, šifro in datumom dokumenta, lastnikom in kratko vsebino, prejemniki tajnega podatka),
- kratek opis okoliščin, v katerih so bili zlorabljeni tajni podatki, in če je znano, število oseb, ki so ali bi lahko imele dostop do tajnega podatka,
- podatek, ali je bil lastnik podatkov obveščen,

- podatke o postopkih in ukrepih, ki so bili izvedeni, da se prepreči nadaljnja zloraba tajnih podatkov.

Če zloraba tajnega podatka kaže na sum storitve kaznivega dejanja, je treba o tem nemudoma obvestiti Policijo ali drug pristojni organ.

Poročilo o kibernetskem incidentu ali napadu na informacijske sisteme, v katerih se obravnavajo tajni podatki, se mora označiti z ustrezno stopnjo tajnosti v skladu z Zakonom o tajnih podatkih. Stopnja tajnosti mora biti enaka stopnji tajnosti zlorabljenih tajnih podatkov.

7 Upravljanje kibernetskih incidentov

Upravljanje kibernetskih incidentov je organiziran sklop ukrepov in aktivnosti, ki so usmerjeni v čim boljšo zaščito, torej preprečevanje nastanka kibernetskih incidentov. Kadar se kibernetski incidenti kljub temu zgodijo, pa je učinkovito upravljanje ključno za čim hitrejšo obnovo omrežij, sistemov in storitev ter normalnega delovanja zavezanca.

Upravljanje kibernetskih incidentov je sestavljeno iz več faz. Za uspešno in učinkovito preprečevanje kibernetskih incidentov ter odzivanje nanje je treba izvajati ukrepe v vseh fazah. Pri tem so nekatere faze ali posamezni ukrepi lahko vključeni kot del drugih faz ali pa so posamezne faze obravnavane hkrati. V posameznih fazah upravljanja kibernetskih incidentov so zapisane osnovne naloge, ki jih mora izvajati zavezanec in ki mora biti pri določanju svojih nalog fleksibilen in jih po lastni presoji lahko razširi.

Faze upravljanja kibernetskega incidenta so:
- Priprava (angl. *Preparation*)
- Zaznavanje (angl. *Detection*)
- Zamejitev (angl. *Containment)*
- Ublažitev (angl. *Mitigation)*
- Obnovitev / okrevanje (angl. *Recovery)*
- Faza zaključka incidenta (angl. *Post incident activities*)

7.1 Faza priprave

To je faza, v kateri se zavezanec pripravlja na neželene dogodke v kibernetskem prostoru. Za učinkovito obvladovanje kibernetskih incidentov so ključni dobra pripravljenost ter predhodna usposabljanja in urjenja v odzivanju na kibernetske incidente. Faza priprav se izvaja samostojno z izdelavo načrtov odzivanja in imenovanjem pristojnih za odzivanje na incidente, z nadgrajevanjem strojne opreme, posodabljanjem programske opreme, usposabljanjem zaposlenih in drugo. Boljše kot so preventivna dejavnost in priprave na področju kibernetske varnosti, boljše in lažje bo odzivanje v vseh naslednjih fazah upravljanja kibernetskih incidentov.

Predvidene osnovne naloge:
- nadgrajevanje strojne in posodabljanje programske opreme,
- usposabljanje zaposlenih s področja kibernetske varnosti,
- ozaveščanje zaposlenih in obveščanje o preteklih kibernetskih incidentih,
- posodabljanje in usklajevanje lastnih varnostnih dokumentov v skladu z dokumenti na državni ravni,
- sodelovanje z URSIV in odzivnim centrom ter
- sodelovanje na državnih ter mednarodnih usposabljanjih in vajah.

7.2 Faza zaznavanja

Faza zaznavanja oziroma identifikacije je faza, v kateri sta ključna pravočasno odkrivanje in prepoznavanje vseh morebitnih kibernetskih incidentov, ki lahko kakor koli škodujejo zavezancu. Pri tem je pomembno zavedanje, da niso vsi kibernetski dogodki tudi kibernetski incidenti, vendar je ključno, da se vse kibernetske aktivnosti v omrežju zaznajo in pravilno opredelijo.

Znake za pojav incidentov razvrščamo v dve skupini, »znanilce« in »kazalnike«. Znanilec je tehnični znak ali dogodek v informacijskem sistemu, da se incident lahko pripeti v prihodnosti, kazalnik pa, da se je incident zgodil ali se dogaja. Na te pojave nas lahko opozarjajo:

- sproženi alarmi (senzorji za preprečevanje in odkrivanje vdorov, zaščita pred škodljivo kodo, sistemi za analizo dnevniških datotek, programska oprema za preverjanje integritete datotek, druge naprave za spremljanje),
- dnevniške datoteke (v operacijskih sistemih, aplikacijah, omrežnih napravah in prometu),
- javno dostopne informacije (informacije o novih ranljivostih in izrabljanjih informacijskega in komunikacijskega sistema),
- osebe ali organizacije (uporabniki, sistemski in omrežni skrbniki sistema, obveščevalno-varnostni organi, druge skupine za odzivanje na računalniške in omrežne incidente).

Zaznavanje kibernetskih dogodkov in identifikacija kibernetskih incidentov temeljita na naslednjih točkah:

- zaznavanje in spremljanje aktivnosti v omrežjih, sistemih in aplikacijah,
- zbiranje situacijskih informacij in odkrivanje nepravilnosti ter zaznavanje negativnega vplivanja,
- izvedba rednega monitoringa sistema in sprotne analize stanja,
- primerne zmogljivosti za odkrivanje kibernetskih incidentov in njihovo upravljanje,
- pravočasno obveščanje odzivnih centrov o kibernetskih incidentih,
- zbiranje in varna hramba dnevniških zapisov in drugih dokazov o kibernetskem incidentu,
- izmenjevanje informacij z zavezanci znotraj sektorja za morebitno dodatno pravočasno odkrivanje enakih ali podobnih kibernetskih incidentov,
- obveščanje javnosti z namenom preprečevanja širjenja ali stopnjevanja kibernetskega incidenta.

Predvidene osnovne naloge:

- prek svojih zmogljivosti informacijske varnosti ali pogodbenih izvajalcev zavezanec spremlja svoja omrežja, sisteme in aplikacije ter zaznava vse nepravilnosti v njih,
- opredeli kibernetski incident ter druge naloge, ki pripomorejo k zaznavanju in identifikaciji kibernetskih incidentov.

Faza zaznavanja je ključna za zavezanca, saj lahko s pravočasno in uspešno zaznavo kibernetskega incidenta začne izvajati primerno in učinkovito upravljanje ter preostale faze upravljanja kibernetskih incidentov. Hitrejši in uspešnejši kot sta zaznava in identifikacija kibernetskega incidenta, boljše bo njegovo nadaljnje upravljanje ter manjše bodo njegove posledice. V tej fazi je zelo pomembno, da se vsi morebitni (digitalni) podatki v zvezi z incidentom, ki se bodo morda uporabili kot dokaz v primeru suma storitve kaznivega dejanja, ustrezno zavarujejo in varno hranijo.

7.3 Faza zamejitve

Po zaznavi in identifikaciji kibernetskega incidenta je ključno njegovo omejevanje, ki pa mora že vsebovati rezultate predtem izvedene analize glede morebitnega vpliva incidenta na omrežje zavezanca in predvidenega medsektorskega vpliva. Glavna prednostna naloga v fazi omejevanja je omejiti vpliv kibernetskega incidenta na omrežja in sisteme zavezanca, preprečevati širjenje incidenta ter omejevati vpliv na storitve zavezanca.

V fazi zamejitve se opravi prva analiza razpoložljivih informacij o kibernetskem incidentu, izvede se primarna ocena nevarnosti in vpliva ter določita primarna stopnja kibernetskega incidenta in prednostno področje upravljanja. V fazi omejevanja se ugotavljajo tudi možni vplivi kibernetskega incidenta na poslovanje in izvajanje bistvenih storitev zavezanca ter se glede na to sprejemajo določeni ukrepi za omejevanje vpliva kibernetskega incidenta.

Omejevanje kibernetskih incidentov temelji na naslednjih točkah:
- spremljanje aktivnosti v omrežjih, sistemih in aplikacijah,
- zbiranje situacijskih informacij in odkrivanje razširjenosti kibernetskega incidenta,
- zbiranje in varna hramba dnevniških zapisov in drugih dokazov o kibernetskem incidentu,
- določanje nevarnosti, vpliva in primarne stopnje kibernetskega incidenta,
- prvo obveščanje odzivnih centrov o kibernetskih incidentih,
- izmenjevanje informacij z zavezanci znotraj sektorja za morebitno dodatno pravočasno odkrivanje enakih ali podobnih kibernetskih incidentov,
- obveščanje javnosti z namenom preprečevanja širjenja ali stopnjevanja kibernetskega incidenta.

Predvidene osnovne naloge:
- prek svojih zmogljivosti informacijske varnosti ali pogodbenih izvajalcev zavezanec spremlja svoja omrežja, sisteme in aplikacije,
- začetek obravnave, primarna ocena nevarnosti in vpliva ter stopnjevanje incidenta,
- prvo poročanje odzivnemu centru,
- zavarovanje ter hranjenje zapisov in dokazov o incidentu,
- po lastni presoji o kibernetskem incidentu obveščanje Policije ter
- izvajanje drugih nalog, ki pripomorejo k zamejitvi kibernetskih incidentov.

Faza omejevanja je pomembna, saj se v tej fazi lahko preprečita širjenje incidenta, njegovo stopnjevanje in zmanjšajo posledice. Uspešnejše je omejevanje kibernetskega incidenta in njegovega vpliva, manjše bodo posledice in škoda, ki jih povzroči kibernetski incident. Faza omejevanja se običajno združi ali tesno povezuje z naslednjo fazo, fazo ublažitve.

7.4 Faza ublažitve

Faza ublažitve je nadaljevanje ukrepov iz faze omejevanja. Fazi omejevanja in ublažitve se običajno prekrivata in dopolnjujeta. V fazi ublažitve se izvajajo ukrepi, ki blažijo vpliv in povzročanje škode na omrežjih, sistemih in aplikacijah zavezanca. Uvedeni ukrepi so odvisni od vrste kibernetskega incidenta in bo za njihovo izvedbo morda potrebno tudi sodelovanje drugih deležnikov - npr. v primeru napada s porazdeljeno ohromitvijo storitve (DDoS, Distributed Denial of Service) bo potrebna podpora ponudnika internetne storitve. V tej fazi je treba izvesti vse aktivnosti, ki pripomorejo k blaženju posledic incidenta, odkrivanju storilca in v nadaljevanju k preprečevanju novih incidentov.

Sprejeti ukrepi v fazi ublažitve so odvisni od vrste incidenta in nevarnosti, ki ga obravnavani incident predstavlja. Določanje ukrepov v fazi ublažitve temelji na naslednjih točkah:
- določanje vzrokov in znakov kibernetskega incidenta za določitev najučinkovitejših ukrepov,
- prepoznavanje, omejevanje ali odstranjevanje programske opreme, ki jo napadalci uporabljajo ali so jo uporabili za izvedbo kibernetskega incidenta (pri tem je ključno, da se ohrani čim več morebitnih dokazov o kibernetskem incidentu, ki bi koristili v predkazenskem postopku),
- priprava za obnovitev z zadnjo čisto varnostno kopijo podatkov (angl. backup),

- določitev storitev, ki so bile uporabljene med kibernetskim incidentom, saj napadalci včasih uporabijo zakonite storitve napadenega sistema.

Predvidene osnovne naloge:
- prek svojih zmogljivosti informacijske varnosti ali pogodbenih izvajalcev zavezanec spremlja svoja omrežja, sisteme in aplikacije,
- nadaljnje upravljanje incidenta,
- stalno ocenjevanje nevarnosti in vpliva ter stopnjevanja incidenta,
- vmesno poročanje odzivnemu centru,
- zavarovanje ter hranjenje zapisov in dokazov o incidentu ter
- druge naloge, ki pripomorejo k ublažitvi kibernetskih incidentov.

Faza ublažitve je nadaljevanje faze omejevanja, torej se nadaljuje preprečevanje širjenje incidenta in njegovega stopnjevanja ter blažijo njegove posledice in morebitna povzročena škoda. Uspešnejše kot je blaženje kibernetskega incidenta in njegovega vpliva, manjše bodo posledice in škoda, ki jo povzroči kibernetski incident, uspešnejša pa bo tudi faza obnovitve oziroma okrevanja, ki sledi.

7.5 Faza obnovitve/okrevanja

Faza okrevanja je namenjena vrnitvi stanja omrežij, sistemov, aplikacij ali storitev v stanje pred kibernetskim incidentom. Ključno je, da se storitve zavezanca začnejo izvajati običajno in nemoteno za uporabnike.

Faza okrevanja se lahko izvede v različnih delih upravljanja kibernetskega incidenta. Če zavezanec lahko storitev opravlja na rezervnem omrežju in izloči napadene dele, potem lahko delno okrevanje storitev izvede takoj, ko je to mogoče, in se z napadenimi sistemi ukvarja v nadaljevanju. V nasprotnem primeru je treba najprej obnoviti omrežje, sistem ali aplikacijo, ki je bila napadena, in šele nato začeti obnavljati storitve na teh sistemih.

Pomembno je, da se z obnovitvijo sistemov, ki so bili vpleteni v kibernetske incidente, ne hiti. Ključno je, da se vse faze in ukrepe izvede temeljito, postopno in dokončno, saj je treba zagotoviti, da so omrežja, sistemi ali aplikacije, preden so dani nazaj v uporabo, zares čisti in varni.

Omrežjem, sistemom ali aplikacijam, ki so vrnjene v uporabo, je treba nameniti posebno pozornost, prav tako kakršnim koli znakom sumljivih kibernetskih aktivnosti, ki jim je treba določiti časovno obdobje z dodatnimi ukrepi za spremljanje.

Predvidene osnovne naloge:
- prek svojih zmogljivosti informacijske varnosti ali pogodbenih izvajalcev zavezanec spremlja obnovljena omrežja, sisteme in aplikacije,
- oceni končni vpliv in posledice incidenta,
- obnovitev sistemov in vrnitev storitev zavezanca v običajno stanje ter
- druge naloge, ki pripomorejo k okrevanju po kibernetskih incidentih.

7.6 Faza zaključka incidenta

Zadnja faza pri upravljanju kibernetskega incidenta se izvede, potem ko je kibernetski incident pod nadzorom, ko so sistemi obnovljeni in storitve povrnjene v normalno stanje. Ta faza se ne sme zanemariti, saj je ključna za učenje iz pridobljenih izkušenj iz upravljanja kibernetskih incidentov.

V tej fazi je treba analizirati, kaj se je zgodilo, vzroke kibernetskega incidenta, kako se je kibernetski incident razvijal med upravljanjem ter vse težave, ki so se pojavile med njegovim upravljanjem. Namen te analize upravljanja kibernetskega incidenta je učenje iz preteklih dogodkov in sprejemanje ustreznih ukrepov za preprečevanje podobnih položajev ter izboljševanje postopkov in ukrepov samega upravljanja incidenta. V tem delu se zaključna faza začne prekrivati s fazo priprav, saj se naučene izkušnje lahko vključijo v varnostno dokumentacijo, ozaveščanje, usposabljanja in vaje.

V zaključni fazi se pripravi tudi podrobno končno poročilo o kibernetskem incidentu, ki zajema tudi oceno škode in stroškov zaradi kibernetskega incidenta ter lahko zajema tudi priporočila ukrepov, ki jih mora zavezanec sprejeti za preprečevanje prihodnjih kibernetskih incidentov.

Predvidene osnovne naloge:

- izvedba podrobne analize kibernetskega incidenta in njegovega upravljanja,
- priprava in pošiljanje zaključnega poročila,
- priprava predloga ukrepov za prenovo ali nadgradnjo strojne in programske opreme,
- priprava predlogov prenove varnostne dokumentacije,
- izmenjava izkušenj o kibernetskem incidentu z odzivnim centrom in URSIV,
- druge naloge, ki so lahko v pomoč v fazi priprav v prihodnje.

8 Zgodovina sprememb dokumenta

Verzija	Datum	Avtor	Opis spremembe
1.0	20.5.2021	Jan Šinigoj	Izdelava dokumenta
2.0	20.8.2023	Jure Šegota	Dopolnitev vsebine (priloge)

Priloga 1: Obrazec za poročanje o kibernetskem incidentu

OBRAZEC ZA POROČANJE O KIBERNETSKEM INCIDENTU

0. Osnovni podatki incidenta

0.1	Referenčna številka incidenta **(Določi odzivni center)**		
0.2	Zadeva	Kratek opis incidenta	
1.5	Poročilo	☐	Prostovoljna priglasitev incidenta
		☐	Prvo poročilo o incidentu zavezanca
		☐	Vmesno poročilo o incidentu zavezanca
		☐	Končno poročilo o incidentu zavezanca

1. Splošne informacije o poročevalcu

1.1	Naziv subjekta, ki poroča	Plinovodi d.o.o.
1.2	Sektor zavezanca	Energetika
1.3	Kontaktni podatki za tehnična vprašanja	Ime priimek, naziv.
		Telefon.
		E-naslov.
1.4	Kontaktna oseba zavezanca	☐ Enaka kontaktni osebi za tehnična vprašanja.
		Ime priimek, naziv.
		Telefon.
		E-naslov.

2. Začetne informacije o incidentu

2.1	Začetek / nastanek incidenta	Datum	hh:mm
	Čas zaznave incidenta v sistemu	Datum	hh:mm
2.2	Opis incidenta	Kratek opis zaznave in trenutne situacije vezane na kibernetski incident.	
2.3	Taksonomija	Klasifikacija incidenta (prva ocena).	
2.5	Ocena stopnje nevarnosti	Primarna ocena stopnje nevarnosti.	Dodaten opis, kaj je potencialno ogroženo (sistem, informacije, storitev,...).
2.6	Ocena možnega vpliva	Primarna ocena možnega vpliva.	Dodaten opis možnega vpliva incidenta (obseg in področje) ter potencialni mednarodni vpliv.

2.7	Ocena stopnje incidenta	Glede na kriterije predlagana ocena stopnje kibernetskega incidenta.
2.8	Opombe	Zapis vseh ostalih podatkov, ki bi lahko koristili v nadaljnjem upravljanju s kibernetskim incidentom.

3. Vmesno / končno poročanje

3.1	Poročilo		☐ Vmesno	☐ Končno
3.2	Čas zadnjega poročanja		Datum	hh:mm.
3.3	Trenutno stanje kibernetskega incidenta		☐ V reševanju	☐ Zaključen
3.4	Opis napake	Tehnični podatki o številu in vrsti sredstev, ki jih je prizadel kibernetski incident (naslovi IP, operacijski sistemi, aplikacije, strežniki in drugo).		
		☐ Okvara sistema	☐ Okvara strežnika	☐ Socialni inženiring
		☐ Zloraba sistema	☐ Zloraba strežnika	☐ Zloraba IP naslova
		☐ Nedelujoče aplikacije	☐ Kraja podatkov	☐ Izsiljevalski virus
		Drugo: Vnos besedila.		
3.5	Izvor incidenta	Vzrok kibernetskega incidenta, če je znan (odpiranje sumljive datoteke, povezovanje USB naprave, dostop do zlonamernega spletnega mesta in drugo).		
		☐ USB ključ	☐ Spletno mesto	☐ Vdor v sistem
		☐ Elektronsko sporočilo	☐ Zlonamerne datoteke	☐
		Drugo: Vnos besedila.		
3.6	Ogrožena storitev zavezanca	☐ Bistvena storitev ZInfV	☐ Ostale storitve	
		Katera bistvena storitev je ogrožena? Vnos.	Katera storitev je ogrožena? /	
		Število prizadetih uporabnikov bistvene storitve: Vnos ocene		
3.7	Taksonomija	Klasifikacija incidenta		
3.8	Stopnja nevarnosti	Stopnja nevarnosti.	Dodaten opis, kaj je napadeno (sistem, informacije, storitev,...).	
3.9	Vpliv incidenta	Vpliv kibernetskega incidenta.	Dodaten opis vpliva incidenta (obseg in področje) ter potencialni mednarodni vpliv.	
3.10	Stopnja incidenta	Glede na kriterije stopnje kibernetskega incidenta.	Stopnja po ZInfV Vstavi	
3.11	Čezmejni vpliv incidenta	Ali ima kibernetski incident vpliv na katero drugo državo (katero, kakšen, kolikšen)?		
3.12	Medpodročni vpliv	Ali ima kibernetski incident vpliv na katero drugo področje (katero, kakšen, kolikšen)?		

		☐DA ☐NE	Če DA, na katero državo, kako in v kolikšni meri?
3.12	Akcijski načrt in protiukrepi	Kateri ukrepi so bili sprejeti za ustavitev širjenja in nadaljevanja kibernetskega incidenta ter kateri ukrepi za odpravo kibernetskega incidenta? Kateri protiukrepi in ukrepi so še načrtovani v nadaljevanju reševanja kibernetskega incidenta?	
		Že sprejeti ukrepi: Vnos besedila.	
		Načrtovani ukrepi: Vnos besedila	
3.13	Povzročena škoda	Ocena materialne škode ali škode povzročene imenu zavezanca.	
3.14	Potrebe za odpravo posledic	Tehnično osebje in tehnična sredstva, ki so potrebna za odpravo incidenta in jih zavezanec neposredno nima na razpolago. Predvideno število dni za odpravo kibernetskega incidenta.	
3.15	Časovni okvir odprave posledic	Ocena, koliko časa po zaključenem incidentu bo zavezanec potreboval, da bo odpravil posledice incidenta ter stanje (sistemov, omrežij, storitev,...) povrnil nazaj v običajno, kot je bilo pred kibernetskim incidentom.	
3.16	Opombe	Zapis vseh ostalih podatkov, ki niso zajeti v zgornjih točkah.	
3.17	Priloge	Seznam priloženih dokumentov, ki bodo pomagali poznati vzrok težave ali njeno razrešitev (posnetki zaslona, datoteke z informacijami, elektronska pošta, »logbooki« in drugo).	
		Vnos besedila.	

PRILOGA 2: Taksonomija kibernetskih incidentov

Kategorija incidenta	Vrsta incidenta	*Incident type*	Opis
Žaljiva/zlonamerna vsebina (Abusive Content)	Neželena sporočila	SPAM	Neželena elektronska pošta vseh oblik, od reklam do zadetkov na loterijah. Prejemnik ni dal preverljivega dovoljenja za pošiljanje sporočila. Sporočilo je poslano kot del večje zbirke sporočil, ki imajo funkcionalno primerljivo vsebino.
	Žaljiva vsebina/žaljiv govor	Harmful Speech	Diskreditacija ali diskriminacija nekoga (npr. kibernetsko zalezovanje, rasizem in grožnje enemu ali več posameznikom).
	Spolna/nasilna vsebina	Child / Sexual / Violence / ...	Otroška pornografija, poveličevanje nasilja in podobno.
Zlonamerna koda (Malicious Code)	Virus	Virus	Programska oprema, ki je namerno vključena ali vstavljena v sistem za škodljive namene. Za aktiviranje kode je običajno potrebna interakcija uporabnika.
	Črv	Worm	
	Trojanski konj	Trojan	
	Vohunska programska oprema	Spyware	
	Dialler	Dialler	
	Rootkit	Rootkit	
	Boti in botneti	Bot	
	Nadzorni strežnik	CnC	
	Izsiljevalski virus	Ransomware	
	Orodje za oddaljeni nadzor (RAT)	Remote Access Trojan	
Zbiranje informacij (Information Gathering)	Odkrivanje morebitnih tarč in ranljivosti	Scanning	Napadi, ki pošiljajo zahteve v sistem za odkrivanje šibkih točk. To vključuje tudi nekakšen postopek testiranja za zbiranje informacij o gostiteljih, storitvah in računih. Primeri: poizvedovanje po DNS, ICMP, SMTP (EXPN, RCPT itd.), skeniranje vrat.
	Prestrezanje komunikacije	Sniffing	Opazovanje in zapisovanje omrežnega prometa (prisluškovanje).
	Socialni inženiring	Social engineering	Zbiranje informacij od posameznika samega na netehnični način (npr. laži, triki, podkupnine ali grožnje).
Poizkusi vdora (Intrusion Attempts)	Izkoriščanje znanih ranljivosti	Exploiting known vulnerabilities	Poskus ogrožanja sistema ali motnje katere koli storitve z izkoriščanjem ranljivosti s standardiziranim identifikatorjem, kot je ime CVE (npr. preliv medpomnilnika, zadnja vrata, skriptno križišče itd.).
	Poskusi prijav, bruteforce in napadi s slovarjem	Login attempts	Več poskusov prijave (Guessing / cracking of passwords, brute force).
	Nova vrsta napada	New attack signatures	Poskusi z neznanim izkoriščanjem.
Vdori (Intrusions)	Zloraba privilegiranega uporabniškega računa	Privileged account compromise	Uspešen vdor v sistem ali aplikacijo (storitve). To lahko na daljavo omogoči znana ali nova ranljivost, pa tudi nepooblaščeni lokalni dostop. Vključuje tudi, da ste del botneta.
	Zloraba neprivilegiranega uporabniškega računa	Unprivileged account compromise	

Kategorija incidenta	Vrsta incidenta	*Incident type*	Opis
	Napadi na aplikacijo	Application compromise	
	Bot	Bot	
Razpoložljivost (Availability)	Napad onemogočanja	DoS	S tovrstnim napadom se sistem bombardira s toliko paketi, da se operacije zavlečejo ali sistem zruši. Primeri DoS so poplave ICMP in SYN, napadi Teardrop in bombardiranje po pošti. DDoS pogosto temelji na napadih DoS, ki izvirajo iz botnetov, obstajajo pa tudi drugi scenariji, kot so napadi z ojačitvijo (DNS Amplification). Na razpoložljivost lahko vplivajo tudi lokalne akcije (uničenje, prekinitev oskrbe z električno energijo itd.) ali višja sila (naravne nesreče), spontane okvare ali človeške napake, ne da bi šlo za zlobo ali grobo zanemarjanje.
	Porazdeljeni napad onemogočanja	DDoS	
	Sabotaža	Sabotage	
	Izpad delovanja naprav ali omrežja	Outage (no malice)	
Varnost informacijskih virov (Information Content Security)	Nepooblaščeni dostop do informacij	Unauthorised access to information	Poleg lokalne zlorabe podatkov in sistemov lahko varnost informacij ogrozi uspešen kompromis med računom ali aplikacijo. Poleg tega so možni napadi, ki med prenosom prestrežejo informacije in dostopajo do njih (prisluškovanje, podvajanje ali ugrabitev). Vzrok je lahko tudi napaka med ljudmi/konfiguracijo/programsko opremo.
	Nepooblaščeno spreminjanje informacij	Unauthorised modification of information	
	Odtekanje informacij	Information disclosure / leakage	
	Uničenje informacij	Information destruction	
Goljufije (Fraud)	Nepooblaščeno izkoriščanje virov	Unauthorized use of resources	Uporaba virov za nepooblaščene namene, vključno s podjetji, ki prinašajo dobiček (npr. uporaba e-pošte za sodelovanje v nezakonitih pismih verig dobička ali piramidnih shemah).
	Intelektualna lastnina in avtorske pravice	Copyright	Ponudba ali namestitev kopij nelicencirane komercialne programske opreme ali drugega materiala, zaščitenega z avtorskimi pravicami (Warez).
	Kraja identitete	Masquerade	Vrsta napadov, pri katerih en subjekt nezakonito prevzame identiteto drugega, da bi imel od tega koristi.
	Phishing sporočilo	Phishing email	Maskiranje v drugo osebo, da bi prepričali uporabnika, da razkrije zasebno poverilnico.
	Phishing spletno mesto	Phishing site	Odkrite lažne spletne strani za izvedbo phishing napada.
	Spletno nakupovanje	On-line shopping	Oškodovanja pri spletnem nakupovanju, lažne spletne trgovine.
	Goljufija z vnaprejšnjim plačilom	Advance-fee fraud	Spletna goljufija, v kateri se zahteva vnaprejšnje plačilo za dostop do obljubljene finančne nagrade ali drugih storitev.
	Izsiljevanje	Extortion	Izsiljevanje z grožnjami objave občutljivih podatkov ali z grožnjami kibernetskega napada.
	Druge goljufije	Scam	Vse druge oblike spletnih goljufij.

Kategorija incidenta	Vrsta incidenta	*Incident type*	Opis
Ranljivost (Vulnerable)	Ranljivi sistemi in naprave	Vulnerable systems	Prosto dostopni in neustrezno zaščiteni sistemi in naprave, ki jih je možno zlorabiti na podlagi znanih ranljivosti. Odprti, nezaščiteni tolmači domenskih imen, svetovno berljivi tiskalniki, ranljivost, ki je razvidna iz pregledov Nessusa, podpisi virusov niso posodobljeni itd.
	Odgovorno razkrivanje	Responsible disclosure	
	Razkritje ranljivosti	Other disclosure	
Drugo (Other)	Drugo	Other	Vse incidente, ki ne sodijo v eno od opredeljenih kategorij, je treba vključiti v ta razred (če se število incidentov v tej kategoriji poveča, to kaže, da je treba sistem klasifikacije spremeniti).
Test	Test	Test	Namenjeno preizkusom.