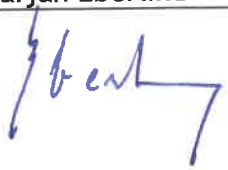
NAČRT ODZIVANJA NA KIBERNETSKE INCIDENTE

Priloga 1: Krizna skupina za odziv na kibernetski incident

IZDELAL	PREGLEDAL	ODOBRIL
Jure Šegota	Jan Šinigoj	Marjan Eberlinc
	 Oton Gortnar 	

1 Namen

Namen dokumenta je določitev krizne skupine za odziv na kibernetski incident, njeno delovanje in sodelovanje z ostalimi deležniki pri zagotavljanju odziva na kibernetski incident.

2 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 vzpostavljen kot Nacionalni odzivni center za kibernetsko varnost (SI-CERT, Slovenian Computer Emergency Response Team).

Družba Plinovodi 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. Priglasitev incidentov lahko izvede kontaktna oseba za informacijsko varnost ali njen namestnik.

2.3 Klasifikacija incidentov

Zaznane kibernetske incidente se klasificira na podlagi spodnjih opisov. Začetno klasifikacijo se izvede glede na prve informacije o incidentu. Glede na kasnejše informacije o obsegu in stanju kibernetskega incidenta se izvaja revizije klasifikacije posameznega kibernetskega incidenta.

STOPNJEVANJE V SKLADU Z ZInfV	STOPNJEVANJE NA PODLAGI KAZALNIKOV	OPIS INCIDENTA
KRITIČNI	KRITIČNI INCIDENT (C1)	Ima velik negativni vpliv na omrežje in informacijske sisteme oziroma informacijske storitve Plinovodov.
TEŽJI	ZELO POMEMBNI INCIDENT (C2)	Zaznan velik negativni vpliv na omrežje in informacijske sisteme oziroma informacijske storitve Plinovodov.
	POMEMBNI INCIDENT (C3)	Možen negativni vpliv na omrežje in informacijske sisteme oziroma informacijske storitve Plinovodov.
LAŽJI	SREDNJI INCIDENT (C4)	Zaznan majhen negativni vpliv na omrežje in informacijske sisteme oziroma informacijske storitve družbe Plinovodi.
	LAŽJI INCIDENT (C5)	Možen vpliv na omrežje in informacijske sisteme oziroma informacijske storitve Plinovodov.
KIBERNETSKA GROŽNJA	VARNOSTNI DOGODEK (C6)	Zaznane kibernetske aktivnosti, ki nimajo vpliva na omrežje in informacijske sisteme Plinovodov.

3 Krizna skupina za odziv na kibernetski incident

3.1 Sestava

Družba Plinovodi ima vzpostavljeno krizno skupino za odziv na kibernetski incident v naslednji sestavi:

- Kontaktna oseba za informacijsko varnost in njen namestnik (koordinacija aktivnosti krizne skupine)
- Skrbnik SUVI
- Skrbnik SUNP
- Vodja Službe za IKT
- Vodja PIS
- Vodja Pravne pisarne
- Direktor tehničnega sektorja
- Skrbnik posameznega prizadetega sistema
- Zunanji izvajalec, ki je vzdrževalec PIS

Krizna skupina lahko po potrebi vključuje tudi ostale zaposlene v družbi Plinovodi ter zunanje izvajalce (npr. VOC) in dobavitelje posameznih prizadetih sistemov.

3.2 Aktivacija krizne skupine

Krizna skupina se aktivira s sklicem krizne skupine, ki jo na podlagi opravljene prve klasifikacije izvede kontaktna oseba za informacijsko varnost ali njen namestnik. V primeru suma na kibernetski incident se na podlagi prvih informacij in pričakovanega obsega incidenta, le tega klasificira v določeno klasifikacijsko skupino (od C1 do C6). Krizna skupina se aktivira za vse incidente, ki so na podlagi osnovnih informacij o incidentu v začetni ali nadaljnjih revizijah klasifikacije ocenjeni z C4 ali višje. Za incidente, ki so klasificirani z oceno C5 in C6, se krizna skupina ne aktivira.

Krizna skupina se po aktivaciji sestane v najkrajšem možnem času, vendar ne kasneje kot v roku 30 minut. Krizna skupina se po aktivaciji fizično sestane v Tehnični sobi MSO, izven delovnega časa pa lahko tudi po drugih komunikacijskih kanalih (MS Teams, telekonferenca,...). Po aktivaciji krizne skupine je potrebno voditi časovno korespondenco vseh dogodkov.

3.3 Pristojnosti krizne skupine

Krizna skupina usmerja vse aktivnosti za omejevanje in odpravo kibernetskega incidenta, vse do vzpostavitve normalnega delovanja omrežja in informacijskih sistemov družbe Plinovodi. Krizna skupina po potrebi vključuje ostale sodelujoče, vse z namenom uspešne zamejitve in odprave kibernetskega incidenta.

Krizna skupina o stanju posameznega kibernetskega incidenta in aktivnostih obvešča poslovodstvo družbe Plinovodi.

4 Zgodovina sprememb dokumenta

Verzija	Datum	Avtor	Opis spremembe
1.0	Oktober 2022	Jan Šinigoj	Izdelava dokumenta
2.0	Maj 2024	Jure Šegota	Dopolnitev vsebine