Plinovodi
Povezani z energijo

OBVESTILA 01/25
Ljubljana, 9. 1. 2025

KROVNA POLITIKA UPRAVLJANJA S POŽARNIMI PREGRADAMI

KROVNA POLITIKA UPRAVLJANJA S POŽARNIMI PREGRADAMI

IZDELAL	PREGLEDAL	ODOBRILA
Jan Šinigoj	Oton Gortnar	Marjan Eberlinc
E-žig ustvarjen za: Jan Šinigoj jan.sinigoj@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 06.01.2025 Potek veljavnosti potrdila: 28.04.2025	E-žig ustvarjen za: Oton Gortnar oton.gortnar@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 06.01.2025 Potek veljavnosti potrdila: 28.04.2025	E-žig ustvarjen za: Marjan Eberlinc marjan.eberlinc@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 08.01.2025 Potek veljavnosti potrdila: 28.04.2025
		Matija Bitenc
		E-žig ustvarjen za: Matija Bitenc Matija.Bitenc@plinovodi.si Napredni e-žig s kvalificiranim potrdilom Imetnik potrdila: mSign Datum e-žiga: 09.01.2025 Potek veljavnosti potrdila: 28.04.2025

Na osnovi določil točk Devetič in Dvanajstič Akta o ustanovitvi družbe z omejeno odgovornostjo PLINOVODI d.o.o., po posredovanju v mnenje Sindikatu delavcev družbe Plinovodi d.o.o. z dne 9. 12. 2024 ter na podlagi sklepa 56. seje Poslovodstva družbe PLINOVODI d.o.o. z dne 19. 12. 2024, sprejme Poslovodstvo družbe Krovno politiko upravljanja s požarnimi pregradami:

1 Namen dokumenta

Namen dokumenta je definiranje krovne politike upravljanja s požarnimi pregradami družbe Plinovodi d.o.o. Družba Plinovodi zagotavlja primarno in sekundarno lokacijo, pri čemer se navedeni dokument nanaša na obe lokaciji družbe in na vse požarne pregrade, ki jih družba uporablja.

2 Krovna arhitektura postavitve

Požarna pregrada mora biti zasnovana v skladu z najboljšimi praksami za varnost omrežij, kar vključuje uporabo robustne arhitekture, ki omogoča visoko razpoložljivost (HA - High Availability) in skladnost s tehničnimi in podatkovnimi zahtevami družbe. Postavitev mora biti prilagojena potrebam družbe in jasnemu poudarku doseganja maksimalne zaščite in razpoložljivosti omrežja. Za zagotavljanje stalne razpoložljivosti in nemotenega delovanja sistema mora biti v konfiguracijo vključen mehanizem visoke razpoložljivosti (HA). Sistem mora biti zasnovan tako, da v primeru okvare ene enote ali omrežne povezave, druga enota samodejno prevzame vse naloge in zagotovi nemoteno delovanje omrežja. Požarna pregrada mora omogočati shranjevanje revizijskih sledi in ločevati internetno omrežje od poslovnega okolja družbe ter procesnega okolja družbe ter ločevati večje število segmentov. Poslovno okolje družbe mora biti s požarno pregrado ločeno od procesnega okolja družbe.

3 Upravljanje s požarnimi pregradami

V vseh primerih upravljanja s požarnimi pregradami je potrebno upoštevati uradna navodila in priporočila proizvajalca opreme ter dejstvo, da mora z opremo, ki je predmet požarne pregrade, rokovati samo ustrezno usposobljeno tehnično osebje.

3.1 Pravila gesel

Vsi uporabniški in administratorski računi na požarni pregradi morajo biti konfigurirani tako, da morajo gesla biti zamenjana vsakih 30 dni. To velja za vse uporabnike z dostopom do požarnih pregrad. Uporabnike se o izteku gesla obvesti 10 dni pred iztekom le tega. V kolikor uporabnik ne zamenja gesla pravočasno se njegov račun samodejno zaklene, dokler gesla ne zamenja, ali dokler skrbnik ne odklene računa. V primeru vpisa pet napačnih gesel se uporabniški račun začasno zaklene.

Pravila za oblikovanje gesel so zasnovana v skladu z najboljšimi varnostnimi praksami in zagotavljajo, da so gesla dovolj močna in varna pred zlorabami. Pravila za gesla so naslednja:

- dolžina gesla: geslo mora biti dolgo vsaj 16 znakov,
- kompleksnost: geslo mora vsebovati najmanj eno veliko črko, eno malo črko, eno številko in en poseben znak,
- ponovna uporaba gesel: prejšnjih gesel ni dovoljeno ponovno uporabljati.

3.2 Beleženje dogodkov in dostopov

Požarna pregrada mora podpirati natančno beleženje dogodkov in dostopov, kar omogoča celovit pregled nad vsemi spremembami v sistemu. Beležiti se morajo naslednji dogodki:

- prijave in odjave: zabeležiti se morajo vsi poskusi prijave in odjave iz sistema, vključno z uporabniškim imenom, datumom in časom,
- spremembe v konfiguraciji: zabeležiti se mora vsaka sprememba v varnostnih pravilih, omrežnih nastavitvah ali politiki dostopov,
- kritične operacije: zabeleženi morajo biti vsi pomembni dogodki, kot so spremembe na požarni pregradi, ustvarjanje ali brisanje uporabniških računov ter spremembe v varnostnih politikah.

Revizijske sledi se morajo hraniti najmanj za obdobje 12 mesecev. Revizijske sledi se morajo hraniti na način, da jih ni mogoče spreminjati. Dostop do revizijskih sledi je omejen na pooblaščene osebe, kar vključuje skrbnike sistema.

3.3 Administrativni dostopi

Dostopi do požarne pregrade morajo biti skrbno dodeljeni na podlagi načel najmanjših privilegijev (Least Privilege Principle) in biti omejeni glede na odgovornosti in potrebe uporabnikov. Uporabniki morajo biti razdeljeni v skupine, ki imajo določene pravice glede na njihove vloge v omrežni infrastrukturi.

3.3.1 Skupine uporabnikov glede na pravice:

- Pravica ''Super uporabnik'' omogoča najbolj obsežne pravice in sicer:
  - popoln dostop do vseh konfiguracijskih nastavitev,
  - dostop do vseh revizijskih sledi,
  - možnost ustvarjanja in spreminjanja uporabnikov in
  - upravljanje nadgradnje in vzdrževanja sistema.

  Zaradi obsežnih pravic, ki jih ima ''Super uporabnik'', je pomembno, da so ti uporabniki skrbno izbrani, da se preprečijo morebitne zlorabe ali napake, ki bi lahko ogrozile varnost omrežja.

- Pravica ''Branje in pisanje'' omogoča popolno konfiguracijo požarne pregrade vendar brez najvišjih administrativnih pravic in sicer omogoča:
  - popoln dostop za branje in pisanje,
  - nastavljanje in prilagajanje varnostnih pravil,
  - spremljanje sistemskih dogodkov in dnevnikov,
  - uporabniške in sistemske nastavitve.

- Pravica ''Branje'' omogoča najnižje pravice dostopa do požarne pregrade in sicer:
  - popoln dostop za branje,
  - pregled dnevnikov in dogodkov.

Uporabniki s tovrstnimi pravicami ne morejo spreminjati ali urejati varnostnih pravil, prilagajati konfiguracijskih nastavitev ali izvajati kakršnihkoli posegov v delovanje požarne pregrade. Njihova vloga je izključno opazovalna.

3.4 Postopek za dodeljevanje in odvzemanje dostopov

Dostopi do požarne pregrade se dodeljujejo in odvzemajo v skladu s formalnim postopkom za upravljanje z dostopi.

3.4.1 Zahtevek za dostop do požarne pregrade

Nov uporabnik (ali uporabnik, ki želi spremembo pravic), ki želi dostopati do požarne pregrade, lahko zaprosi za dostop izključno preko formalnega postopka, to je z oddajo vloge za dostop do požarne pregrade, pri čemer pravice uporabnika določi glede na njegove odgovornosti.

3.4.2 Odobritev dostopa do požarne pregrade

Vsako vlogo za dostop do požarne pregrade mora odobriti Vodja Službe za informacijsko-komunikacijske tehnologije oziroma njegov pomočnik ali Vodja oddelka PIS. Šele po odobritvi se zagotovi dostop do požarne pregrade.

3.4.3 Periodični pregledi dostopov

Dostope do požarne pregrade je potrebno redno pregledovati, najmanj na vsake 3 mesece, da se zagotovi, da imajo uporabniki ustrezne pravice glede na njihove naloge in pristojnosti. Pregled dostopov se ustrezno zabeleži. Skrbnik požarne pregrade mora voditi ažurirani seznam oseb, ki imajo dostop do požarne pregrade.

3.5 Postopek za upravljanje s pravili na požarni pregradi

Pred posodobitvijo pravil ali konfiguracijo novih pravil na požarnih pregradah mora vzdrževalec sistema pridobiti odobritev izvedbe. Za namen odobritve izvedbe mora vzdrževalec sistema pristojnim v odobritev posredovati zahtevek, v katerem navede

potrebne spremembe in razlog zanje ter potencialna tveganja, ki bi jim družba lahko bila podvržena zaradi sprememb.

Pristojni za odobritev posodobitve pravil ali odobritev konfiguracije novih pravil na strani družbe Plinovodi so:

- Vodja Službe za informacijsko-komunikacijske tehnologije,
- Pomočnik vodje Službe za informacijsko-komunikacijske tehnologije,
- Vodja Oddelka PIS.

Brez pisne odobritve vzdrževalec požarne pregrade ne sme posodobiti pravil ali konfigurirati novih pravil. Vsako posodobljeno ali novo konfigurirano pravilo na požarni pregradi mora imeti zabeležen razlog kreiranja oziroma spremembe.

Izjema pri odobritvi pravil so morebitna izjemno visoka tveganja oziroma stanja v fazi kibernetskega napada ali poskusa kibernetskega napada, kjer lahko vzdrževalec požarne pregrade vpeljuje nova pravila in konfigurira obstoječa pravila z namenom takojšnjega zmanjšanja tveganj. O tem mora vzdrževalec požarne pregrade čimprej obvestiti pristojne za odobritev pravil na strani družbe Plinovodi.

4 Uveljavitev

Ta politika začne veljati in se uporablja od objave v Obvestilih.

Ljubljana, dne 6. 1. 2025

Glavni direktor
Marjan Eberlinc, univ. dipl. inž . str.

E-žig ustvarjen za:
Marjan Eberlinc
marjan.eberlinc@plinovodi.si

Napredni e-žig s kvalificiranim potrdilom
Izdajatelj potrdila: mSign
Datum e-žiga: 08.01.2025
Potek veljavnosti potrdila: 28.04.2025

Namestnik glavnega direktorja
mag. Matija Bitenc, univ. dipl. ekon.

E-žig ustvarjen za:
Matija Bitenc
Matija.Bitenc@plinovodi.si

Napredni e-žig s kvalificiranim potrdilom
Izdajatelj potrdila: mSign
Datum e-žiga: 09.01.2025
Potek veljavnosti potrdila: 28.04.2025