Plinovodi
Povezani z energijo

OBVESTILA 12/23

Ljubljana, 12. 9. 2023

Strategija kibernetske varnosti družbe Plinovodi d.o.o.

Plinovodi
Povezani z energijo

STRATEGIJA KIBERNETSKE VARNOSTI DRUŽBE PLINOVODI D.O.O.

Ljubljana, september 2023

Na podlagi določil točk Devetič in Dvanajstič Akta o ustanovitvi družbe z omejeno odgovornostjo je Poslovodstvo družbe Plinovodi d.o.o. dne 4. 9. 2023 sprejelo

STRATEGIJO KIBERNETSKE VARNOSTI DRUŽBE PLINOVODI D.O.O.

ki določa poglavitne usmeritve na področju kibernetske varnosti družbe.

V družbi Plinovodi izvajamo obvezno državno gospodarsko javno službo operaterja prenosnega sistema plina v Republiki Sloveniji (RS), ki je regulirana s strani Agencije za energijo. Zaradi specifične dejavnosti družbe, ki deluje odgovorno do uporabnikov sistema in v javnem interesu, po modelu neodvisnega operaterja prenosnega sistema, je ključni poudarek družbe na varnem, zanesljivem in gospodarnem obratovanju ter razvoju prenosnega sistema plina in zagotavljanju kakovostnih, preglednih in nepristranskih storitev za uporabnike sistema. Na podlagi energetske zakonodaje mora operater prenosnega sistema še posebej varovati zaupnost poslovno občutljivih podatkov, ki jih dobi med izvajanjem svoje poslovne dejavnosti ter preprečevati diskriminatorno razkrivanje poslovno koristnih podatkov o svojih dejavnostih.

Sodoben poslovni svet je tesno povezan z naprednimi informacijskimi tehnologijami, dostopnimi in hitrimi komunikacijami ter naprednimi izmenjavami podatkov. Varnost informacijskih in komunikacijskih sistemov (IK infrastruktura ali IK sistemi) je ključna za zagotavljanje vseh funkcij operaterja prenosnega sistema skladno z zakonodajo. Napredek informacijsko komunikacijskih tehnologij (IKT) zahteva njihovo stalno spremljanje in ustrezno prilagajanje družbe, ob tem pa omogoča inovativne načine rabe tehnologij in različne razvojne priložnosti na informacijsko komunikacijski ravni. Obseg in pomen uporabe IK infrastrukture v družbi se povečuje in posledično se povečuje tudi pomen IKT za stabilno in kakovostno poslovanje družbe.

V dokumentu je kibernetska varnost opredeljena skladno z evropsko[1] in nacionalno zakonodajo (Zakon o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 - ZEKom-2, 18/23 - ZDU-1O in 49/23) oziroma strategijo o kibernetski varnosti RS[2]).

---

[1] DIREKTIVA (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. decembra 2022 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2).

[2] Kibernetska varnost je v Strategiji kibernetske varnosti RS opredeljena kot:

- skupek aktivnosti in drugih ukrepov, tehničnih in ne-tehničnih, katerih namen je zaščititi računalnike, računalniška omrežja, strojno in programsko opremo ter informacije, ki jih le-ta vsebuje in obravnava, kar vključuje programsko opremo in podatke kot tudi druge elemente kibernetskega prostora, pred vsemi grožnjami, vključno z grožnjami nacionalni varnosti;
- stopnja zaščite, ki jo aktivnosti in ukrepi lahko zagotovijo;
- združena področja profesionalnih naporov, vključno z raziskavami in razvojem na področju implementiranja in izboljševanja ukrepov ter dvigovanja kakovosti le-teh.

Vizija kibernetske varnosti družbe

V družbi sledimo razvoju informacijskih tehnologij in se ob tem zavedamo, da razvoj informacijskih tehnologij poleg prednosti prinaša tudi tveganja vse bolj naprednih in sofisticiranih kibernetskih groženj. Zavedamo se, da je popolno varnost pred kibernetskimi napadi, zlorabami, goljufijami, napakami človeške in tehnološke narave ter drugimi vplivi nemogoče absolutno zagotoviti. Cilj družbe je z vrsto preventivnih ukrepov in sistemov zmanjšati tveganje vseh navedenih groženj na sprejemljivo raven. Z namenom minimaliziranja tovrstnih tveganj strategija kibernetske varnosti narekuje izvajanje ukrepov skladno z najvišjimi standardi kibernetske varnosti. Visoko stopnjo kibernetske varnosti bomo dosegali z optimalno izrabo zmožnosti obstoječih tehnologij in procesov ter z vpeljavo novih, naprednejših in učinkovitih tehnologij in z ustrezno varnostno ozaveščenostjo zaposlenih. Pri razvoju in implementaciji sistemov za višanje stopnje kibernetske varnosti bomo primarno črpali znanje in izkušnje iz lastnih visoko usposobljenih kadrov ter dodatno vključevali zanesljive in strokovno preizkušene zunanje izvajalce na nivoju najboljše razpoložljive tehnologije in znanja (BAT). Zagotovili bomo, da bo preprečevanje varnostnih incidentov obsegalo vsebinsko od tehnične zasnove komponent IK sistemov do ozaveščenosti uporabnikov in upoštevanja predpisov, ki pripomorejo k razvoju varnejših sistemov, upravljanju z njimi ter prepoznavi in odzivu na grožnje. Z namenom zagotavljanja najvišje stopnje strokovnosti vpeljave IK sistemov bomo redno letno izvajali periodična neodvisna varnostna preverjanja. Ob tem bomo zagotavljali tudi ustrezno varovanje osebnih podatkov posameznika[3] ter upoštevali standarde, ki zagotavljajo varno in nemoteno delovanje sistemov.

Zaradi vsega navedenega v družbi zagotavljamo celovit sistem kibernetske varnosti, ki naslavlja vse njene aspekte, s posebnim poudarkom na ravnanju zaposlenih in ustreznem varovanju vstopnih točk v informacijski sistem družbe. Vzpostavljeni sistemi družbe zagotavljajo varen prenos podatkov in izmenjavo informacij z uporabniki sistema in vsemi ostalimi deležniki na nacionalni ravni, kakor je to določeno z zakonodajo. Pristojnim inštitucijam za kibernetsko varnost bomo poleg obstoječih informacij zagotavljali tudi vse potrebne podatke za prihodnji razvoj v smeri globalizacije kibernetske varnosti in z njimi aktivno sodelovali.

Z zagotavljanjem ustrezne stopnje kibernetske varnosti bomo zagotovili stabilno delovanje IK infrastrukture, pomembne za delovanje družbe, in s tem razpoložljivost sistemov in podatkov. Strategijo kibernetske varnosti družbe obravnavamo kot del poslovne strategije družbe.

Strateški cilji kibernetske varnosti družbe

Za sledenje viziji družbe Plinovodi na področju kibernetske varnosti smo si postavili naslednje strateške cilje:

1. družba zagotavlja neprestano (24/7) spremljanje kibernetskih incidentov,

[3] UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) in Zakon o varstvu osebnih podatkov (ZVOP-2) (Uradni list RS, št. 163/22)

2. družba odgovorno skrbi za kibernetsko varnost IK sistemov ob upoštevanju ekonomske upravičenosti na nivoju reguliranih energetskih podjetij,
3. družba uvaja učinkovite in priznane ter preizkušene sisteme kibernetskega varovanja skladno z njihovim razvojem in dostopnostjo,
4. družba zagotavlja uporabo sistemov, ki so sposobni hitrega zaznavanja in odzivanja na varnostne grožnje, ter predstavljajo učinkovito zaščito IK infrastrukture, s čimer je zagotovljeno neprekinjeno obratovanje prenosnega sistema ter poslovanje družbe,
5. z namenom izmenjave informacij med deležniki sodelujemo z njimi na državnem nivoju in skladno z zakonodajo,
6. družba načrtuje in uvaja IK infrastrukturo skladno s stanjem razpoložljive in preizkušene tehnike tako, da zagotavlja varno in nemoteno delovanje sistemov s poudarkom na zagotavljanju zasebnosti posameznika,
7. družba podpira vzpostavitev visoke informacijsko varnostne kulture zaposlenih preko rednih izobraževanj in ozaveščanja zaposlenih.

Izvajanje strateških ciljev kibernetske varnosti družbe

Zagotavljanje kibernetske varnosti družbe je že del aktivnosti delovanja obstoječe IK infrastrukture in tudi njenega razvoja. Vizijo in strateške cilje kibernetske varnosti družbe pa bomo dosegali z naslednjimi ukrepi:

- razvojem IK infrastrukture družbe z uvajanjem novih tehnologij za izboljšanje kibernetske varnosti,
- ustrezno zaščito komunikacijskih poti pred vstopom v informacijski sistem družbe,
- vzpostavitvijo mehanizmov preventivnega delovanja, ki bodo grožnje in napake v največji meri preprečevali,
- zagotavljanjem ustreznih postopkov in mehanizmov odzivanja na incidente ter stalno posodabljanje in izboljševanje postopkov odzivanja glede na pretekle izkušnje,
- spodbujanjem uporabe standardov na področju kibernetske varnosti, vključno s standardi za procesne tehnologije,
- izvajanjem redne ocene tveganj IK sistemov ter na podlagi rezultatov načrtovanje ustreznih ukrepov za zaščito pred tveganji oziroma zmanjševanjem le teh,
- izvajanjem rednih letnih notranjih presoj SUVI in SUNP,
- izvajanjem ozaveščanja in izobraževanj zaposlenih v družbi, s čimer bomo zmanjševali tveganja in gradili informacijsko varnostno kulturo,
- sledenjem pravnim okvirjem kibernetske varnosti v RS in EU ter izpopolnjevanjem sistemov družbe,
- rednim izvajanjem testiranj neprekinjenega delovanja sistemov ter na podlagi analiziranja rezultatov oblikovanje predlogov za izboljšanje delovanja,
- rednimi neodvisnimi zunanjimi in notranjimi varnostnimi skeniranji in vdornimi testiranji IK sistemov,
- stalnim izboljševanjem kibernetske drže z odpravo prepoznanih pomanjkljivosti IK sistemov preko incidentov, varnostnih testov ali drugih virov,
- zagotavljanjem ključnih podatkov in IK sistemov na primarni in sekundarni lokaciji družbe,

- uporabo naprednih mehanizmov in naprav za varovanje podatkov in informacij družbe,
- seznanjanjem in ozaveščanjem vseh zaposlenih s strategijo kibernetske varnosti in spodbujanjem k njenemu uresničevanju,
- spodbujanjem zaposlenih, posebej pa vodij k aktivnostim za minimaliziranje tveganj na področju IK sistemov

V družbi Plinovodi bomo z izvajanjem ukrepov strategije kibernetske varnosti skladno z nacionalno strategijo in zakonodajo tudi v prihodnje zagotavljali zanesljivost delovanja in povečevali stopnjo kibernetske varnosti informacijskih in komunikacijskih sistemov pri upravljanju prenosnega sistema.

Strategija kibernetske varnosti družbe Plinovodi je strateški dokument, ki je načelno in krovno vodilo razvojnih aktivnosti za zagotavljanje kibernetske varnosti. Izvajanje strategije bo prilagojeno razpoložljivim sredstvom v okvirih aktualnih finančnih načrtov družbe.

Ta Strategija kibernetske varnosti družbe Plinovodi stopi v veljavo, ko jo sprejme Poslovodstvo ter se objavi v Obvestilih družbe. Z dnem uveljavitve te Strategije kibernetske varnosti družbe Plinovodi preneha veljati Strategija kibernetske varnosti družbe Plinovodi z dne 21. 4. 2022 (Obvestila 02/22).

Marjan Eberlinc
glavni direktor