STALIŠČE AGENCIJE ZA ENERGIJO #3/2018

KIBERNETSKA VARNOST

Agencija za energijo (v nadaljevanju agencija) v okviru svojih nalog med drugim seznanja deležnike v energetskem sektorju s trendi na področju kibernetske varnosti in dejavnostmi, ki so v okviru Evropske unije in izven njenih meja povezane s tem področjem. Cilj agencije je strokovno prispevati k usmerjanju predvsem izvajalcev gospodarske javne službe (GJS) k stroškovno učinkovitim naložbam na področju zagotavljanja kibernetske varnosti[1].

Operativna vloga agencije je sicer zaenkrat v kontekstu kibernetske varnosti v glavnem osredotočena na nadzor kakovosti oskrbe z energijo in s tem povezanih izpadov, ki so lahko posledica kibernetskih dejavnosti. S temi aktivnostmi je povezana temeljna naloga agencije, in sicer priznavanje upravičenih stroškov naložb in spremljanje oziroma vrednotenje le-teh bodisi na podlagi dolgoročnejših razvojnih načrtov bodisi kratkoročnejših naložbenih načrtov elektroenergetskega sistema in sistema zemeljskega plina.

V kontekstu kibernetske varnosti izvajalcev GJS v energetskem sektorju se agencija pri prepoznavanju nalog izvajalcev kritičnih oziroma bistvenih storitev primarno osredotoča na zakonodajni okvir, določen z Energetskim zakonom (v nadaljevanju EZ-1). Le-ta v členih 54 in 78 izvajalcem GJS distribucije in prenosa električne energije oziroma v členih 177 in 216 operaterju prenosnega sistema in operaterjem distribucijskega sistema zemeljskega plina nalaga zagotavljanje varnega, zanesljivega in učinkovitega obratovanja in vzdrževanja prenosnega oziroma distribucijskega sistema ter njun razvoj ob upoštevanju zahtev varnega in zanesljivega obratovanja sistemov. Stališče agencije je, da v okvir te opredelitve sodi izvajanje ustrezne informacijske varnosti oziroma kibernetske zaščite. Agencija se zaveda, da je verjetnost udejanjenja kibernetskih groženj sicer majhna, vendar lahko ima za sistem in končne uporabnike občutne kolateralne posledice. Posledično agencija pričakuje, da so vse naložbe v kibernetsko oziroma informacijsko varnost načrtovane in koordinirane, usklajene s pristojnimi organi[2], predvsem pa da so stroškovno kratkoročno in dolgoročno učinkovite.

Agencija v prihodnje pričakuje bolj konstruktivno obravnavo stroškovnega načrtovanja za upravljavce kritične infrastrukture in izvajalce bistvenih storitev, ki izvajajo GJS, in sicer z vsemi nosilci in upravljavci sektorjev v energetskem sistemu pri pripravi in ažuriranju dokumentov načrtovanja zaščite kritične infrastrukture, ki

[1] Temo kibernetske varnosti konkretneje obravnavamo polletno v okviru Slovenskega energetskega varnostnega foruma (SEVF), na katerem se srečujemo z izvedenci s področja poslovne in procesne informatike izvajalcev gospodarske javne službe (v nadaljevanju GJS) z elektroenergetskega področja.
[2] Ministrstvo za infrastrukturo, Ministrstvo za obrambo, pristojni nacionalni organ za informacijsko varnost, nacionalni odzivni center za kibernetsko varnost

ga nalaga ZKI[3], in nadzorstev ter sistemskega pristopa kibernetske zaščite, ki ga nalaga ZInfV[4].

Agencija meni, da je treba vzpostaviti tesnejše sodelovanje pri obveščanju med pristojnimi organi, saj bo le na ta način agencija lahko učinkovito izvajala regulacijo. Po načelu potrebe po seznanitvi pričakujemo tudi obveščanje agencije o stalnih in dodatnih ukrepih, ki jih strokovno usmerja in usklajuje Ministrstvo za obrambo in jih nalaga ZKI, ter obveznostih in ukrepih v okviru ZInfV, ki jih strokovno usmerja in usklajuje pristojni nacionalni organ za informacijsko varnost. Nenazadnje se morajo omenjeni ukrepi zrcaliti v razvojnih in naložbenih načrtih operaterjev. Pri njihovem potrjevanju agencija utemeljeno pričakuje boljšo koordinacijo in sodelovanje s pristojnimi organi.

Usklajeno in sistematično načrtovanje kibernetske varnosti se mora kazati v čim večji stroškovni učinkovitosti. Mnenje agencije je, da je treba upoštevati načela celovitega pristopa, s stalnim načrtovanjem zaščite ter izmenjave podatkov in informacij kot tudi posvetovanja med deležniki, predvsem pa sistematičnost pri naložbah v informacijsko (kibernetsko) varnost upravljavcev kritične infrastrukture in izvajalcev bistvenih storitev v energetskem sektorju.

Agencija meni, da je smotrno in najučinkoviteje izhodiščne rešitve za izvajanje informacijske varnosti in kibernetske zaščite iskati v obstoječih kadrovskih virih in ciljnih operativnih skupinah znotraj naslovljenih izvajalcev GJS. Le-ti naj delujejo v navezavi z nacionalnim odzivnim centrom za kibernetsko varnost, pristojnim nacionalnim organom za informacijsko varnost in preverjenimi zunanjimi izvajalci, ki imajo na področju informacijske varnosti in kibernetskega varovanja večletne operativne izkušnje.

Maribor, oktober 2018

[3] Zakon o kritični infrastrukturi (Uradni list RS, št. 75/17)
[4] Zakon o informacijski varnosti (Uradni list RS, št. 30/18)