SAMORKA

Samorka eru samtök orku- og veitufyrirtækja á Íslandi. Innan samtakanna starfa fráveitur, hitaveitur, vatnsveitur, raforku–framleiðendur, raforkusalar og flutnings- og dreifingaraðilar raforku

Reykjavík, 14. janúar 2019

Alþingi
Nefndarsvið
101 Reykjavík

Efni: Umögn Samorku um frumvarp til laga um öryggi net og upplýsingakerfa mikilvægra innviða. Þingskjal 557 - 416. mál. 149. löggjafarþing 2018-2019.

Samorka tekur undir mikilvægi þess að sett séu lög um öryggi net- og upplýsingakerfa mikilvægra innviða.

Öll aðildarfélög Samorku falla undir skilgreiningu frumvarpsins um rekstraraðila nauðsynlegra þjónustu og þar með mikilvægra innviða. Allir íbúar landsins og öll fyrirtæki njóta þjónustu aðilafélaganna, hverja klukkustund, allan sólahringinn, alla daga ársins. Öryggi orkuframleiðslu, rafmagns og jarðhita, flutnings- og dreifikerfa, rafmagns, heita vatnsins og neysluvatnsins, eru þannig ómissandi grunnur að daglegu lífi íbúa og rekstri fyrirtækja.

Síðastliðið sumar komu fram drög að framangreindu frumvarpi og voru þau lögð inn á Samráðsgátt stjórnvalda til umsagnar. Samorka skilaði inn mjög ítarlegri umsögn og gerði alvarlegar athugasemdir við mjög margt í frumvarpsdrögunum. Því er **mjög jákvætt** að sjá að **tekið hefur verið tillit til** mjög margra þeirra **athugasemda og ábendinga** sem komu fram í umsögn okkar.

Engu að síður viljum við vekja athygli á nokkrum atriðum sem áður hafa verið gerð að umtalsefni í umsögn okkar.

Í greinargerð með frumvarpinu er í 6. kafla fjallað um mat á áhrifum þess og segir m.a. svo.

> „Verði frumvarp þetta að lögum er ljóst að lagðar verða kröfur á mikilvæga innviði um ákveðið skipulag á öryggi net- og upplýsingakerfa þeirra; umgjörð áhættustýringar og viðbúnaðar, og eftirlitsstjórnvöldum falið eftirlit með framkvæmd ákvæða þeirra hverju á sínu sviði. Hér eru því lagðar íþyngjandi kröfur á viðkomandi aðila að viðlögðum viðurlögum. Kröfurnar byggja á hinn bóginn á mikilvægum almannahagsmunum, þ.e. sjónarmiðum um að samfélags- og efnahagslega mikilvæg þjónusta njóti lágmarksverndar gegn utanaðkomandi ógnum. Mikilvægum innviðum er jafnframt tryggður aðgangur að mikilvægri þjónustu og aðstoð af hálfu öryggis- og viðbragðsteymis Póst- og fjarskiptastofnunar vegna netógna og atvika (netöryggissveit). Fá þeir aðgang að sólarhringsþjónustu sveitarinnar sem hefur stöðu CSIRT-teymis á Íslandi; aðgengi að hópi sérfræðinga og með óbeinum hætti í gegnum þá sérfræðinga upplýsingar eða viðvaranir um ógnir sem einungis sambærileg teymi alþjóðlega hafa aðgang að.“

Í framangreindri umsögn Samorku um frumvarpsdrögin var bent á mikilvægi þess að meta með hvaða hætti hægt sé að **draga úr kostnaði við opinbert eftirlit** (þar með talið kaupum og rekstri á eftirlitsbúnaði) með samvinnu við netöryggissveitir á Norðurlöndunum og þá mögulegum samningum um útvistun verkefna. Ljóst er að mjög dýrt er að koma þessum búnaði upp og sömuleiðis að uppfæra hann til að halda í við hraða tækniþróun sem ekki sér fyrir endann á. Með sama hætti er mjög kostnaðarsamt að þjálfa starfsfólk, viðhalda þekkingu þess og halda því í starfi.

Í frumvarpinu er einnig gert ráð fyrir að um kostnaðarauka verði að ræða hjá einstökum eftirlitsstjórnvöldum sem í tilviki orku- og veitugeirans eru Orkustofnun og Umhverfisstofnun. Með þetta í huga er mikilvægt að huga að öllum leiðum sem geta dregið úr kostnaði. Auk framangreindrar ábendingar um samstarf við Norðurlöndin má einnig benda á eftirfarandi.

Í lagafrumvarpinu er á nokkrum stöðum fjallað um mikilvægi þess að fyrirtækin komi sér upp virku innra eftirliti fyrir öryggi net- og upplýsingakerfa. Þetta eru allt eðlilegar og sjálfsagðar kröfur og innra eftirlitið jafnan hluti af vottuðum gæðakerfum viðkomandi fyrirtækja í orku- og veitugeiranum. Því er mikilvægt í þessu samhengi að nota þetta tækifæri til þess að árétta og ítreka að slíkt innra eftirlit sem er viðurkennt og reglulega tekið út og vottað af ytri eftirlitsaðila á jafnframt að skapa tækifæri til þess að draga úr og einfalda opinbera eftirlitið. Á þessu vöktum við athygli í umsögn okkar um frumvarpsdrögin s.l. sumar. Mikilvægt er að um þetta sé fjallað með **jákvæðu ákvæði í lögunum og þar með opnað á þennan möguleika**, þ.e. að heimilt sé að uppfylla kröfur laganna með tilvísun til vottaðs innra eftirlits.

Eins og áður segir verða samkvæmt frumvarpinu lagðar miklar kröfur á mikilvæga innviði um öryggi net- og upplýsingakerfa þeirra, skipulag, umgjörð, áhættustýringu og viðbúnað, ásamt viðamiklu eftirliti.

Í III. kafla frumvarpsins er fjallað um þetta eftirlit, um eftirlitsstjórnvöld og eftirlitsheimildir. Í VI. kafla er síðan fjallað um viðurlög við brotum umræddum lagagreinum, þ.e. II. kafla og 19. gr.

Í viðurlagakaflanum er svo annars vegar fjallað um stjórnsýsluúrræði, þ.e. dagsektir, en hins vegar refsingar, þ.e. fangelsi og sektir. Þessu til viðbótar er síðan í 5. mgr. 12. gr. gert ráð fyrir að eftirlitsstjórnvald geti látið þriðja aðila vinna verk á kostnað viðkomandi fyrirtækis (mikilvægs innviðs), sem felur í sér að viðunandi úrbætur séu gerðar á öryggi net- og upplýsingakerfa fyrirtækisins og þá væntanleg á grundvelli rökstuddrar niðurstöðu rannsóknar þar að lútandi.

Ekki er gott að átta sig á samspili þessara stjórnvaldsúrræða og framkvæmdar þeirra. Þeim verður þó væntanlega ekki beitt samtímis og gera verður ráð fyrir að hægt sé að bera hvor tveggja undir dómstóla, en ekki aðeins dagsektarákvörðunina, sbr. 2. mgr. 22. gr. Er full ástæða til að taka af tvímæli um þetta í lagatextanum.

Þá er með hliðsjón af efni II. kafla og þeim skyldum sem þar eru lögð á fyrirtækin (mikilvæga innviði) ekki auðvelt að sjá fyrir sér með hvaða hætti einstaklingar (starfsmenn fyrirtækjanna) baki sér refsiábyrgð samkvæmt lögunum. Lítið er fjallað um þetta í greinargerð með 23. gr. laganna, aðeins sagt að *„tilskipun (ESB) 2016/1148 geri ráð fyrir að viðurlög við brotum gegn ákvæðum hennar séu skilvirk, í réttu hlutfalli við brotið og beitt þannig að hafi varnaðaráhrif.“* Í tilskipuninni er fjallað um þetta í 21. gr. undir fyrirsögninni „penalties“ sem hér merkir væntanlega viðurlög í víðum skilningi, fremur en fangelsisrefsingu eina og sér, ef marka má samhengið í greininni. Sjá hér t.d. leiðbeiningar breskra yfirvalda um innleiðingu á NIS tilskipuninni frá apríl 2018. Er því ástæða til þess að rýna þetta frekar og leita eftir atvikum til sérfróðra aðila á sviði refsiréttar í því skyni. Ber í þessu sambandi einnig að benda á að í nefndu ákvæði, 21. gr. tilskipunarinnar, er sérstaklega tekið fram að viðurlög skuli vera í réttu hlutfalli við brotið.

Áréttað er að Samorka er almennt mjög hlynnt innleiðingunni og meginn tilgangi lagafrumvarpsins enda um mjög mikilsverða hagsmuni að tefla að net- og upplýsingaöryggi mikilvægra innviða séu ávallt í fyrirrúmi í rekstri þeirra. Fullyrða má að öll stærstu fyrirtækin innan Samorku hafa unnið markvisst í þessum málum nú þegar. Þá eru mörg þeirra jafnframt hluti af stærri rekstraheildum þar sem sérstaklega er unnið að þessum málum (innan sveitarfélaga). Þá má minna á að stærstu fyrirtækin innan Samorku hafa samstarf innan Neyðarstjórnar Raforkukerfisins (NSR) og á vettvangi Netöryggishóps Samorku þar sem hægt er að vinna að stefnumótun í málaflokknum og deila þekkingu og reynslu. Má í þessu sambandi benda á norrænar fyrirmyndir t.d. KraftCert í Noregi.

Um leið og SAMORKA þakkar þetta tækifæri til þess að koma að umsögn um málið, viljum við áretta að fá að gera það áfram í ferli málsins fyrir Alþingi.

Að öðru leyti vísar SAMORKA til umsagna einstakra aðildarfyrirtækja.

Virðingarfyllst,

f.h. Samorku – samtaka orku- og veitufyrirtækja

Páll Erland framkvæmdastjóri