



Samgöngu- og sveitarstjórnarráðuneytið
snr@srn.is
Mál nr. S-79/2018

Reykjavík, 15. ágúst 2018.

Umsögn ISNIC

um drög að frumvarpi til laga um öryggi net- og upplýsingakerfa mikilvægra innviða

Inngangur.

Tilefni frumvarpsins er svokölluð NIS-tilskipun Evrópusambandsins. Samt sem áður er frumvarpið að mörgu leyti veigameira og setur þyngri skyldur og byrðar varðandi eftirlit en tilskipunin gerir, án þess að rök séu færð fyrir þörf á þyngra eftirliti með netumferð á Íslandi, en í löndum Evrópusambandsins. Þá virðist sem ríkið ætti sér með frumvarpinu að yfirtaka stóran hluta af þeim markaði, sem einkafyrtæki á sviði netöryggis og -eftirlits sjá nú um, með því að þvinga hlutaðeigandi til að gera þjónustusamninga við ríkisrekinn eftirlitsaðila. ISNIC hefur ekki fundið slíku ákvæði, þ.e.a.s. skyldu til að gera saminga, stað í NIS-tilskipuninni.

Internet á Íslandi hf, ISNIC, er virkur meðlimur í CENTR, samtökum rekstraraðila höfuðléna, einkum í Evrópu (The Concil of European National Top Level Domain Registries), sem nú telur um 55 meðlimi í Evrópu, auk rekstraraðila í Ástralíu, Íran, Ísrael, Japan og Canada. CENTR samtökin komu, ásamt sérfræðingum nokkurra meðlima þess, að gerð þess hluta NIS-tilskipunarinnar sem fjallar um öryggi rekstraraðila landshöfuðléna. Umsögn CENTR (sjá hlekk neðst) var höfð til hliðsjónar við skrif þessarar umsagnar.

Meðlimir CENTR, þ.m.t. ISNIC, líta á öryggismál sem forgangsmál. Þess vegna fagnar ISNIC þeim þáttum í frumvarpinu sem eiga sér stoð í NIS-tilskipuninni og lúta að því að efla öryggisvitund fyrirtækja og almennings, auka traust og samstarf milli landa, auka traust og samstarf milli stofnana, auka samstarf milli CERT hópa (netöryggissveita) og síðast en ekki síst milli rekstraraðila netkerfa innanlands sem utan.

Hins vegar hefur ISNIC áhyggjur af því að frumvarpið, með sínu séríslenska sniði og mjög íþyngjandi ákvæðum um gerð rekstrarsaminga um stöðugt rafrænt eftirlit, muni-þvert á markmið þess-beinlínis draga úr áhuga og þátttöku netfyrirtækja til að vinna saman að annars ágætu netöryggi landsins.

ISNIC bendir löggjafanum góðfúslega á að frumvarpið er ólíkt NIS-tilskipuninni, sem kveður á um *létt eftirlit sem framkvæmt skuli eftir á*, en í 60. formálslið hennar segir: *Digital service providers should be subject to light-touch and reactive ex post supervisory, justified by the nature of their service and operations.* Andi NIS-tilskipunarinnar er þannig jákvæður gagnvart aðilum hennar, enda er henni ætlað að efla öryggisvitund og samstarf aðildarríkja og fyrirtækja á sviði netöryggismála til langa tíma. Að mati ISNIC verður það ekki gert með valdi eingöngu.

Stöðugu eftirliti með netumferð sbr. 19. gr. frumvarpsins hafnað.

Mikilvægur þáttur í starfsemi ISNIC er reksturinn á RIX (Reykjavík Internet Exchange) en „Rixinn“, eins og þjónustan er kölluð, kemur í veg fyrir að innlend internetnotkun flæði að óþörfu um útlandasambönd með tilheyrandi kostnaði og töfum. Vert er að taka fram að ISNIC rekur Rixinn án hagnaðarmarkmiðs til hagsbóta fyrir innlent netsamfélag. Sjá nánar á RIX.is.

Í 19. gr. frumvarpsins er gert ráð fyrir að Rixinn sé nauðsynlegur innviður (sem hann er ekki) og að eftirlitsaðilinn fái heimild til að setja upp búnað hjá rekstraraðilanum (ISNIC), sem hlustar á alla netumferð sem um hann flæðir. Þessu hafnar ISNIC alfarið og mun leggja þjónustuna niður verði frumvarpið að lögum óbreytt.

- Í fyrsta lagi hafnar ISNIC þessu af prinsipp-ástæðum og með hliðsjón af eigin upplýsingastefnu og trúverðugleika félagsins.
- Í öðru lagi vegna þess að þjónusta nettengipunkta sem reknir eru á sömu forsendum og RIX, er ekki nauðsynleg til þess að umferð flæði milli aðila sem þeim tengjast. Lokist IX-þjónusta leitar umferð milli aðila annað á sjálfvirkan hátt. Þess vegna ætti Rixinn ekki að teljast til nauðsynlegrar þjónustu sbr. 5. gr. frumvarpsins.
- Í þriðja lagi hafnar ISNIC hugmyndum um sjálfvirk og viðvarandi neteftirlit vegna þess að tæknilega ómögulegt er að koma á sjálfvirku stöðugu eftirliti með netumferð með því að tengja búnað við Rixinn eins og hann er. Slík hlustun myndi eyðileggja rekstur RIX.is, sem byggir á afkastamíklum tengingum gegn mjög lágu aðildargjaldi.
- Í fjórða lagi gengur ákvæði frumvarpsins gegn NIS-tilskipuninni, þveröfugt við það sem segir í skýringum með frumvarpinu. Sjá 60. formálslið tilskipunarinnar, sem gerir ráð fyrir að eftirlit verði léttvægt (e. *light touch*) og skuli viðhaft eftir að atvik koma upp (e. *reactive ex-post*).

Sú fullyrðing í umfjöllun í greinargerð um 1. mgr. 19. gr. frumvarpsins, að ákvæðið sé til staðar svo hún [Netöryggissveitin] geti sinnt því hlutverki sem krafist er samkvæmt 2. lið viðauka I við tilskipunina, er **röng**. Í viðauka I undir lið 2 (a)(i) stendur á ensku: *monitoring incidents at a national level* og undir lið (ii) *providing early warning, alerts... about risks and incidents.* Þetta þýðir á íslensku, að mati ISNIC, að fylgjast [skuli] með atvikum og senda snemma (ekki samtímis) út aðvaranir um atvik og áhættur. Að mati ISNIC felst ekki í þessu heimild til að fylgjast með netumferð almennt og stöðugt allan sólarhringinn.

Allir sem til þekkja vita hvernig umræðan var í aðdraganda NIS-tilskipunarinnar. Ákvæði líkt og haldið er fram í greinargerð frumvarpsins að finna megi í tilskipuninni, hefði aldrei verið samþykkt af CENTR eða netsamfélagini, sem haft var með í ráðum við gerð hennar, eins og áður hefur komið fram.

ISNIC sendi Patrik Fållstrom, tæknilegum framkvæmdastjóra Netnod í Stokkhólmi, og þekktum stjórnanda í alþjóðlega netsamfélagini, sem rekur stærsta internetskiptipunktinn á Norðurlöndum, spurningar 9. ágúst sl. um hvort tengipunktur Netnod heyrði undir NIS-tilskipunina og hvort Netnod þyrti að hýsa búnað sem hlustaði á netumferðina um hann, eins og 19. gr. frumvarpsins segir til um. Skemmt er frá því að segja að Patrik sendi strax eftifarandi svar sem birt er hér með hans leyfi:

Tilvitnun hefst.

„In Sweden the implementation just like the directive say that services covered by the implementation of the Electronic Communications Directive 2002/58/EC. As IX:es are covered in Sweden, it is excluded from the implementation of the NIS directive.

I am curious though, what part of the NIS directive do give the right for the regulator to investigate the traffic? In Sweden traffic (and traffic patterns) is still to be kept secret according to implementation of 2002/58/EC and the right for law enforcement (for example) to investigate it is implemented as exceptions.

*Patrik Fältström
Technical Director and Head of Security"
Netnod.se*
Tilvitnun lýkur.

ISNIC hvetur til að viðeigandi breytingar verði gerðar á frumvarpinu og að „tengi- og skiptipunktar (RIX eins og hann er) verði ekki skilgreindir almennt sem rekstraraðili nauðsynlegrar þjónustu sbr. 5. gr. frumvarpsins og vísar þar til ákvæða 2. liðar a og c í 5. gr. NIS-tilskipunarinnar um að þjónustan þurfi að vera nauðsynleg í þjóðfélagini (a) og um að atvik verði að valda verulegum truflunum (c). Hvorugt er að mati ISNIC fyrir hendi. ISNIC sér heldur ekki að NIS-tilskipunin heimili almennt og stöðugt eftirlit með netumferð.

Um 3. gr. Gildissvið.

Í greininni eru örfélög eða lítil félög, eins og venja er með íþyngjandi lög, undanskilin lögunum. Hins vegar er orðasambandið „stafrænir þjónustuveitendur“ notað í stað orðsins „félög“. Bent skal á þetta hér.

Um 19. og 20. grein.

ISNIC er sammála því að til að fá fram hröð og góð viðbrögð við öryggisatvikum þurfi upplýsingaflæði frá rekstraraðilum nauðsynlegrar þjónustu (RNÞ) að vera gott og hratt. Þó verður að hafa eftirfarandi grundvallaratriði í huga:

1. Að innihaldi netumferðar verði hvorki safnað né sent, heldur einungis umferðarupplýsingar (flow-accounting, meta-data).
2. Að aldrei verði komið upp búnaði undir stjórn 3ja aðila (í þessu tilfelli netöryggissveitar) á netum RNÞ. Verði það gert opnast nýr möguleiki á netöryggisbrotum, sem RNÞ hefur ekki stjórn á, t.d. ef brotist er inn í eftirlitsbúnað, sem staðsettur er á neti RNÞ.

Breyta þarf 19. og 20. grein frumvarpsins til að taka af öll tvímæli um þetta.

Fleira verður ekki tínt til í bili. Sumarleyfi starfsmanna ISNIC settu strik í reikninginn við gerð umsagnarinnar og því var beðið um frest út ágústmánuð, en þeirri beiðni var hafnað. Þó var fresturinn lengdur um 3 virka daga og fyrir það skal þakkað.

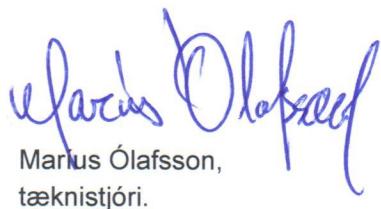
Virðingarfyllst,

f.h. Internet á Íslandi hf. ISNIC

Jens Pétur Jensen,
framkvæmdastjóri.

Umsögn CENTR um NIS-tilskipunina:

<https://centr.org/members-library/library/policy-document/centr-opinion-on-the-draft-eu-nis-directive.html?filtersub=CENTR%20comment>


Marius Ólafsson,
tæknistjóri.