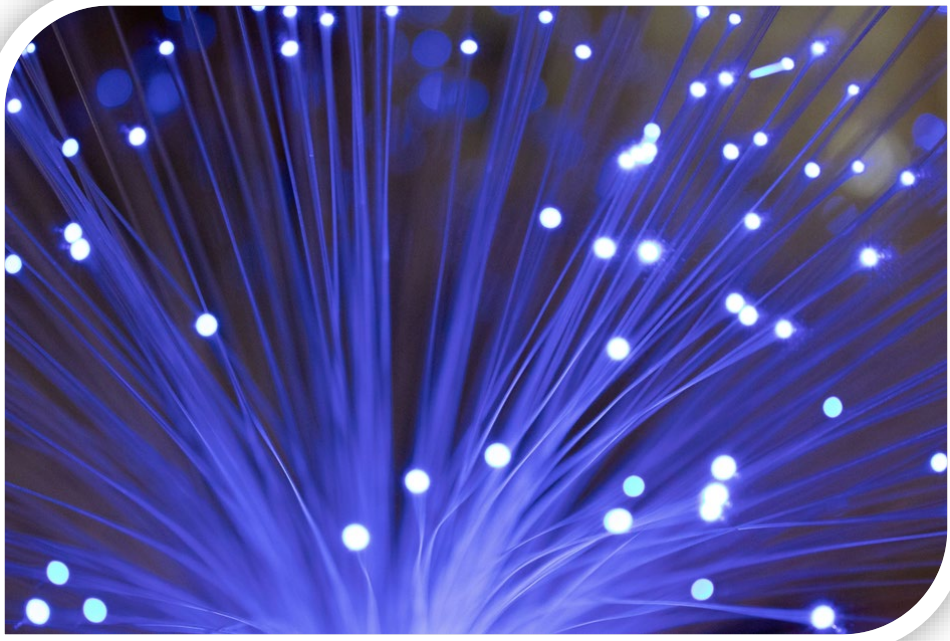
Stefna Póst- og fjarskiptastofnunar

um öryggi og virkni fjarskiptainnviða



Póst- og fjarskiptastofnun
MARS 2020

Efnisyfirlit

Formáli

Fjarskipti og fjarskiptaþjónusta af ýmsu tagi gegnir mikilvægu hlutverki í því nútíma þjóðfélagi sem Ísland er. En landið er nú í efsta sæti þjóða heims á einkunnalista Alþjóðafjarskiptasambandsins samkvæmt skýrslu sem birt var í nóvember 2017 um stöðu og þróun upplýsingasamfélagsins og fjarskipta í heiminum. Þetta sýnir að staða upplýsingatækni og fjarskipta hér á landi gegnir mikilvægu hlutverki í efnahagslegu og samfélagslegu tilliti. Þetta er jákvæð staðreynd og þróun en hefur jafnframt í för með sér nýjar og krefjandi áskoranir.

Öryggi og virkni fjarskiptaþjónustu og fjarskiptaneta eru grundvallarforsenda þess að upplýsingasamfélagið viðhaldist og þróist frekar sem megininnviður í þjóðfélaginu. Enn fleiri rekstraraðilar nauðsynlegrar þjónustu reiða sig á upplýsingatækni og fjarskipti í rekstri sínum og með innkomu nýrrar háraða farnetstækni, 5G mun þessi þróun einungis halda áfram og á áður óþekktum hraða. Það er því eðlilegt að aukin krafa sé gerð til öryggis og virkni fjarskiptaneta.

Póst- og fjarskiptastofnun, sem eftirlitsstjórnvald á svið fjarsktipa, hefur haft hlutverk hvað þetta varðar um alllangt skeið og viðhaft eftirlit með hvort tveggja öryggi og meðferð fjarskiptaupplýsinga sem og raunlægu og kerfislægu öryggi fjarskiptaneta. Stofnunin telur, á grundvelli þess aukna þunga sem hvílir á öryggi og virkni almennra fjarskiptaneta, nauðsynlegt að setja sérstaka stefnu hvað þetta varðar. Þá er ljóst að ný fjarskiptalöggjöf Evrópusambandsins kveður á um ítarlegri kröfur á þessu sviði.

Í þessu stefnuskjali verður gerð grein fyrir framtíðarsýn stofnunarinnar hvað þetta eftirlitshlutverk varðar. Þessi framtíðarsýn byggir í fyrsta lagi á ákveðnum **almennum markmiðum** stofnunarinnar sem felast í að i) öðlast yfirsýn og styrkja með heildstæðum hætti *öryggisstig almennra fjarskiptaneta og almennrar fjarskiptaþjónustu, þ.m.t. fjarskiptaleynd,* sem og ii) í að öðlast yfirsýn og efla *virkni og þanþol* (e. recilianse) almennra fjarskiptaneta hér á landi.

Í öðru lagi byggir sýn stofnunarinnar á **sértækari markmiðum** sem sett eru til að vinna að því að hin almennu markmið náist. Slík sértækari markmið ná þá til frekari útfærsluþátta almennu markmiðanna, svo sem hvernig stofnunin hyggst stuðla að *eflingu öryggisstigs* almennra fjarskiptaneta og –þjónustu og hvernig hún mun reyna að stuðla að *virkni og auknu þanþoli*, fjarskiptaneta og -þjónustu á einstökum hlutum netanna eða á sérstökum þjónustusvæðum. Stærsta verkefni slíkra sértækra markmiða er að hvetja fjarskiptafyrirtækin til að auka öryggisvitund sína sem og að setja fram úttektaráætlun fyrir stofnunina.

Þá er í stefnunni fjallað í stuttu máli um þróun innan Evrópusambandsins er varðar öryggi 5G neta sem og nýtt samevrópskt vottunarferli sem verið er að setja á stofn hjá Netöryggisstofnun Evrópu (ENISA).

Drög að þessari stefnu fóru í opið samráð í nóvember 2019. Ekki bárust veigamiklar athugasemdir frá hagsmunaaðilum og eru stefnan því efnislega samhljóða samráðsskjalinu.

1. Hlutverk Póst- og fjarskiptastofnunar

Póst- og fjarskiptastofnun hefur umsjón með fjarskiptum hér á landi og hefur eftirlit með framkvæmd laga um fjarskipti. Fjarskiptalög kveða á um margvíslegar skyldur á aðila sem reka fjarskiptanet og veita almenna fjarskiptaþjónustu. Þannig ber þeim fjarskiptafyrirtækjum sem veita almenna fjarskiptaþjónustu að gera viðeigandi ráðstafanir til að tryggja öryggi þjónustunnar í samráði við rekstraraðila fjarskiptaneta ef við á. Þeim ber að tryggja fjarskiptaleynd, þ.e. að verja upplýsingar sem fara um fjarskiptanet gegn því að þær glatist, skemmist eða breytist fyrir slysni eða að óviðakomandi fái aðgang að þeim. Eins ber þeim að gera sérstakar ráðstafanir til að tryggja samfelldan og órofinn rekstur almennra fjarskiptaneta. Er sett sérstök krafa á fjarskiptafyrirtæki um að skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, framkvæma áhættumat og ákveða öryggisráðstafanir á grundvelli þess.

Um framangreint er fjallað í 47. gr. fjarskiptalaga nr. 81/2003, sem og reglum sem Póst- og fjarskiptastofnun hefur sett með stoð í 2. og 3. mgr. ákvæðisins. Um er að ræða reglur nr. 1221/2007, um vernd upplýsinga á almennum fjarskiptanetum og reglur nr. 1222/2007, um virkni almennra fjarskiptaneta. Í ákvæði 47. gr. sem og í framangreindum reglum Póst- og fjarskiptastofnunar er að finna frekari útlistun á þeim kröfum sem hvíla á fjarskiptafyrirtækjum hvað öryggi upplýsinga og virkni neta varðar.

Þar er jafnframt að finna ákveðnar lágmarkskröfur sem gerðar eru til þeirra, eftir því sem við á. Ábyrgðin á fjarskiptaleynd og öryggi og virkni fjarskiptaneta hvílir ávallt á viðkomandi fjarskiptafyrirtæki. Þannig ber fyrirtækið ábyrgð á gerð áhættumats og á þeim öryggisráðstöfunum sem það hefur valið m.t.t. greindrar áhættu sem steðjar að öryggi og virkni fjarskiptanetsins og fjarskiptaþjónustunnar. Þá eru settar fram ýmsar kröfur um gerð neyðaráætlunar, innra eftirlit og endurskoðun á öryggisskipulaginu.

Póst- og fjarskiptastofnun hefur eftirlit með framkvæmd fjarskiptalaga og þar á meðal framangreindum ákvæðum og reglum. Hér er um að ræða hvort tveggja raunlægt eftirlit, þ.e. eftirlit með áþreyfanlegum og efnislegum hlutum og raunverulegu umhverfi, sem og kerfislægt eftirlit. Hefur stofnunin heimild til að kalla eftir upplýsingum og framkvæma, eða láta framkvæma, úttektir til að kanna hlítni fjarskiptafyrirtækja við umræddar kröfur. Framkvæmd tæknilegs eftirlits getur verið með ýmsum hætti, t.a.m. að meta hlítni við lagakröfur með almennum hætti yfir markaðinn, að leiðbeina aðilum við að uppfylla kröfurnar og með framkvæmd úttekta.

Stofnunin hefur fram til þessa staðið að úttektum á ýmsum afmörkuðum fjarskiptainnviðum og meðferð upplýsinga.[1] Þá hefur hún jafnframt rannsakað mál ef upp hefur komið öryggisatvik. Það mat stofnunarinnar nú að þörf sé á að setja fram markvissari stefnumótun og áætlun á þessu sviði. Að mati stofnunarinnar er nauðsynlegt að nýta aðrar tegundir eftirlitsúrræða en einungis úttektir til að öðlast hvort tveggja yfirsýn yfir stöðu öryggisskipulags á markaðinum almennt sem og að auka samvinnu og traust milli stofnunarinnar og markaðsaðila á þessu sviði.

[1] Það eftirlit byggir reyndar á 42. gr. fjarskiptalaga sem fjallar sérstaklega um gögn um fjarskipti sem fjarskiptafyrirtækjum er skylt að geyma í sex mánuði.

2. Fjarskiptaleynd og virkni almennra fjarskiptaneta

2.1 Almennt

Ákvæði um vernd upplýsinga og virkni almennra fjarskiptaneta og almennrar fjarskiptaþjónustu hafa verið í gildi frá árinu 2007. Það var hins vegar árið 2009 sem að evrópsku fjarskiptalöggjöfinni var breyt og sambærileg ákvæði komu þar inn. Ákvæði fjarskiptalaga byggðu þó á evrópskri fyrirmynd en ákveðnar öryggiskröfur höfðu áður verið til staðar í tilskipun á sviði persónuverndar. Þannig hafa ákvæði íslensku löggjafarinnar ekki byggt með beinum hætti á samevrópsku regluverki á sviði fjarskipta en þau eru að mjög miklu leiti efnislega sambærileg.

Í desember á síðasta árið samþykkti Evórpuþingið og ráðið nýja heildarlöggjöf á sviði fjarskipta í Evrópu, þ.e. tilskipun (EU) 2018/1972.[2] Nú er unnið að innleiðingu þessarar tilskipunar í íslenskan rétt og samkvæmt þingmálaskrá ríkisstjórnarinnar fyrir 150. löggjafarþing (2019-2020) hyggst samgöngu- og sveitarstjórnarráðherra leggja fram frumvarp til innleiðingar á tilskipuninni á vorþingi. Í þessari tilskipun er að finna nokkuð ítarleg ákvæði er varðar öryggi og virkni almennra fjarskiptaneta og almennrar fjarskiptaþjónustu. Byggja þau þó áfram á þeirri aðferðarfræði sem fyrri tilskipanir, og fjarskiptalög, byggja á. Þótt vissulega felist ákveðnar breytingar í hinni nýju löggjöf má að töluverðu leyti líta til núgildandi ákvæða og framkvæmdar. Verður í þessum kafla farið yfir núgildandi ákvæði fjarskiptalaga og þær kröfur sem hvíla á fjarskiptafyrirtækjum en vert er að hafa í huga komandi breytingar.

2.2 Öryggi upplýsinga á almennum fjarskiptanetum

Í IX. kafla laga nr. 81/2003, um fjarskipti er fjallað um vernd persónuupplýsinga og friðhelgi einkalífsins. Er í 42. gr. laganna fjallað um gögn um fjarskipti, meðferð þeirra og eyðingu þeirra. Fjallar ákvæðið í fyrsta lagi um eyðingu og geymslu fjarskiptaumferðarupplýsinga, sbr. 1.-3. og 7. mgr. ákvæðisins, og í öðru lagi um vinnslu þeirra, sbr. 4.-6. mgr. ákvæðisins og byggir að mestu leyti á 6. gr. tilskipunar Evrópuþingsins og Ráðsins 2002/58/EB um vinnslu persónuupplýsinga og um verndun einkalífs á sviði rafrænna fjarskipta.

Fyrsta málsgrein 42. gr. felur í sér þá meginreglu að fjarskiptafyrirtækjum er skylt að eyða gögnum um fjarskiptaumferð eða gera þau nafnlaus þegar þeirra er ekki lengur þörf við afgreiðslu ákveðinnar fjarskiptasendingar. Frá þessari kröfu er þó að finna tvær undanþágur. Í fyrsta lagi þá er fjarskiptafyrirtækjum heimilt að geyma þau gögn sem nauðsynleg eru til reikningsgerðar fyrir áskrifendur og uppgjörs fyrir samtengingu þar til ekki er lengur hægt að vefengja reikning eða hann fyrnist, sbr. 2. mgr. ákvæðisins. Í öðru lagi er fjarskiptafyrirtækjunum skylt, í þágu rannsókn sakamála og almannaöryggis, að varðveita ákveðna lágmarksskráningu gagna um fjarskiptaumferð í sex mánuði, sbr. 3. mgr. ákvæðisins.

Í 26. gr. inngangsorða tilskipunarinnar kemur einnig fram að gögn um áskrifendur, sem notuð eru á rafrænum fjarskiptanetum til að koma á tengingum og til að senda upplýsingar, innihalda upplýsingar um einkalíf einstaklinga og snerta rétt þeirra til að samskiptin séu bundin trúnaði eða þau snerta réttmæta hagsmuni lögaðila. Kemur líka fram að slík gögn megi aðeins geyma að því marki sem nauðsynlegt er til að veita þjónustuna, gefa út reikninga og innheimta gjöld fyrir samtenginu og einungis í takmarkaðan tíma. Samkvæmt 29. lið inngangsorðanna er fjarskiptafyrirtækjum þó heimilt að vinna umferðargögn um áskrifendur í einstökum tilvikum

[2] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance. Sjá: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN

og eins þau umferðargögn sem nauðsynleg eru vegna útgáfu reikninga til koma upp um og stöðva svik sem felast í ógreiddri notkun rafrænu fjarskiptaþjónustunnar.

Þannig er markmið 42. gr. að tryggja einkalíf áskrifenda með sem bestum hætti og er, að mati Póst- og fjarskiptastofnunar, nauðsynlegt að samlesa ákvæðið með tilliti til 47. gr. fjarskiptalaga en saman er þessum ákvæðum ætlað að tryggja fjarskiptaleynd.

Í 1. mgr. 47. gr fjarskiptalaga er sett fram sú krafa á fjarskiptafyrirtæki, sem veita almenna fjarskiptaþjónustu, að þau geri viðeigandi ráðstafanir til þess að tryggja öryggi þjónustunnar. Þá skulu þau jafnframt verja upplýsingar sem fara um fjarskiptanet gegn því að þær glatist, skemmist eða breytist fyrir slysni eða að óviðkomandi fái aðgang að þeim. Er hér um að ræða inntak upplýsingaöryggis sem felst í því að tryggja leynd upplýsinga, lögmætan aðgang að þeim, aðgengi þeirra og réttleika.

Til þess að unnt sé að meta gæði upplýsingaöryggis er nauðsynlegt að fyrir liggi skrifleg lýsing á fyrirkomulagi þess samkvæmt ákveðinni aðferð. Þannig er kveðið á um það í 2. mgr. ákvæðisins að fjarskiptafyrirtæki skuli skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, framkvæma áhættumat og ákveða öryggisráðstafanir á grundvelli þess. Þá hefur Póst- og fjarskiptastofnun, líkt og áður seigr, jafnframt sett reglur um vernd upplýsinga í almennum fjarskiptanetum, sbr. reglur nr. 1221/2007 þar sem fjallað er með nokkuð ítarlegum hætti um kröfur á fjarskiptafyrirtæki varðandi upplýsingaöryggi.

Reglurnar ná til fjarskiptafyrirtækja sem reka fjarskiptaþjónustu í almennum fjarskiptanetum og gilda um almenn fjarskiptanet. Þeim er ætlað að tryggja fjarskiptaleynd, réttleika upplýsinga og öryggi þeirra. Er í 7. gr. reglnanna sett fram sú krafa að fjarskiptafyrirtæki skuli útbúa og viðhalda skjalfestri lýsingu á stjórnkerfi sem tryggir upplýsingaöryggi í fjarskiptaþjónustu og fjarskiptanetum. Þá er tilgreint í 1.-3. tl. hvað skuli að lágmarki felast í slíku stjórnkerfi, þ.e.:

1. *Fjarskiptafyrirtæki skal setja sér skriflega öryggisstefnu. Í henni skal m.a. koma fram almenn lýsing á afstöðu æðsta stjórnanda fjarskiptafyrirtækis til öryggismála. Í stefnunni skulu koma fram markmið og meginreglur upplýsingaöryggis samkvæmt rekstrarstefnu og rekstrarmarkmiðum. Stefnan skal kynnt öllum starfsmönnum fjarskiptafyrirtækisins sem hafa með fjarskiptarekstur að gera. Við mótun öryggisstefnu skal taka mið af því hvaða upplýsingar skuli vernda, hvernig skuli vernda þær, þeirri aðferð sem viðhöfð verður við vinnslu þeirra og hver beri ábyrgð á öryggi þeirra. Skal öryggisstefnan birt starfsmönnum.*
2. *Fjarskiptafyrirtæki skal skilgreina aðferðarfræði áhættumats um upplýsingaöryggi og henni fylgt eftir með skriflegu áhættumati um upplýsingaöryggi sem tengist fjarskiptanetum og fjarskiptaþjónustu. Áhættumat skal bera kennsl á áhættuþætti, umfang þeirra og forgangsraða þeim miðað við ásættanlega áhættu og þau markmið sem skipta máli fyrir fyrirtækið. Áhættumat skal skilgreina eignir og gera á þeim einfalt mat og mat á þeim áhrifum sem myndast af völdum rofs á leynd, réttleika og tiltækileika. Miklir veikleikar og ógnir eru skilgreind fyrir eignirnar, ásamt mati á líkindum þeirra. Áhættan fyrir hvert atriði er reiknuð út og hún borin saman við fyrirframgerðan mælikvarða um ásættanlegt áhættustig um öryggi upplýsinga, órofinn rekstur og þjónustustig. Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum og skal það endurskoðað reglulega.*

3. *Fjarskiptafyrirtæki skulu setja sér verklagsreglur um örugga meðferð upplýsinga og eyðingu þeirra. Gerðar skulu öryggisráðstafanir og settar fram skriflegar lýsingar á þeim. Tilgreina skal hvaða öryggisráðstöfunum verði beitt og hvernig þær verði útfærðar, þ. á m. við hönnun, þróun,* rekstur, prófun og viðhald hvers kerfis. Þá skal og tekið fram hvernig brugðist verði við áföllum í rekstri fjarskiptaneta og fjarskiptaþjónustu. Öryggisráðstafanir skal endurskoða reglulega. Skriflegar leiðbeiningar skulu vera til staðar fyrir einstaka ferla sem nauðsynlegir eru fyrir upplýsingaöryggi fjarskiptaneta og fjarskiptaþjónustu. Fjarskiptafyrirtækið skal sjá til þess að ákvæðum stefnunnar um upplýsingaöryggi sé framfylgt, líka þegar verktakar vinna fyrir fyrirtækið. Fjarskiptafyrirtækið skal sjá til þess að starfsmenn þess framfylgi stefnunni um upplýsingaöryggi.

Þá er jafnframt gerð krafa um að til staðar sé virkt innra eftirlit til að tryggja að unnið sé í samræmi við öryggisstefnu og skjalfestar verklags- og öryggisreglur sem og að til staðar sé áætlun um samfelldan rekstur (viðbragðsáætlun) sem er ætlað að tryggja öryggi upplýsinga ef til þjónusturofs kemur. Eins er að finna ákvæði í reglunum er varðar lágmarksráðstafanir vegna starfsmenn, þ.e. til að fyrirbyggja og takmarka tjón vegna mistaka, svika og annarrar misnotkunar. Þá skal viðhafa ákveðnar aðgangsstýringar og nauðsynlegar tæknilegar og skipulagslegar ráðstafanir til að verja almenn fjarskiptanet.

Í reglunum er einnig að finna ákvæði er varðar útvistun reksturs fjarskiptaneta. Kemur þar fram að stjórnunarlegri ábyrgð og áhættustýringu verður ekki útvistað og að skilyrði fyrir gerð slíks samnings sé að fjarskiptafyrirtæki hafi staðreynt að umræddur aðila hafi sett sér öryggisstefnu og geti framkvæmt nauðsynlegar öryggisráðstafanir samkvæmt reglunum.

2.3 Virkni almennra fjarskiptaneta

Í gildi hér á landi er einnig nokkuð umfangsmikið regluverk er varðar virkni almennra fjarskiptaneta og er það jafnframt eitt af hlutverkum stofnunarinnar að tryggja að heildstæði og öryggi almennra fjarskiptaneta sé viðhaldið. Í 3. mgr. 47. gr. fjarskiptalaga kemur fram að sérstakar ráðstafanir skulu gerðar til að tryggja samfelldan og órofinn rekstur almennra fjarskiptaneta og hefur stofnunin sett reglur nr. 1222/2007, þar um.

Í reglunum er kveðið á um þær lágmarks ráðstafanir sem Póst- og fjarskiptastofnun telur nauðsynlegt að fjarskiptafyrirtækin geri til að tryggja samfelldan rekstur almennra fjarskiptaneta og raunlæga vernd þeirra. Þá er sérstaklega tilgreint að þær kröfur sem ekki koma beint fram í reglunum skulu fyrirtækin sjálf bera kennsl á með skipulegu áhættumati og viðhafa aðgerðir til að stýra og stjórna fjarskiptanetum með tilliti til áhættu, sbr. 4 .gr. reglnanna. Er fjarskiptafyrirtækjum þannig gert að nýta sér áhrifagreiningu og áhættumat til að draga úr öllum stærri veikleikum og veilum í innviðum sínum. Eins skulu þau gera neyðaráætlun sem byggir á þeirri niðurstöðu áhættumats, sbr. í 7. gr. reglnanna en í 4. og 5. mgr. greinarinnar segir:

> *Í áhættumati skal greina sérstaklega alla mikilvæga innviði. Lýsa skal notkun á mikilvægu innviðunum og samtengingum þeirra við aðra hluta fjarskiptanetsins og við önnur fjarskiptanet. Ennfremur skal lýsa hvernig öryggi mikilvægu innviðanna er tryggt á besta mögulega hátt, þ.m.t. vernd gegn straumrofi, upplýsinga- og vöktunarkerfi, aukaleiðir, viðbragðsbúnaður, þjónustusamningar, vernd gegn öryggisatvikum, raunlæg vernd og hvernig er staðið að öryggisafritun.*

Við gerð áhættumats skal fylgja að öðru leyti þeim leiðbeiningum sem fram koma í 7. gr. reglna Póst- og fjarskiptastofnunar nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum.

Framangreint felur í sér að fjarskiptafyrirtæki hafa lögbundna skyldu til að framkvæma áhættumat, skilgreina mikilvægi innviði sína og tryggja kerfsilæga og raunlæga vernd þeirra með sérstökum öryggisráðstöfunum. Þá skulu fyrirtækin jafnframt setja sér neyðaráætlun, þ.e. ráðstafanir til að tryggja samfelldan og órofinn rekstur, sem byggir á niðurstöðum áhættumatsins og lýtur virku innra eftirliti.

Í reglunum er sérstaklega um raunlæga vernd fjarskiptarýma, fjarskiptabúnaðar og fjarskiptalagna. Er kveðið á um ákveðnar lágmarksráðstafanir sem skulu viðhafðar eftir því sem við á. Þá er gerðar ákveðnar kröfur um virkni, þ.m.t. til afkastagetu og rekstraröryggi flutningsleiða, afkastagetu og rýmd búnaðar sem, afkastagetu fastlínusímaneta sem og annarra almennra fjarskiptaneta. Þá er að finna ákvæði er varða stjórn almennra fjarskiptaneta, búnað þeirra og högun, umferðarstýringar og viðhald.

Ljóst er af framangreindu að nokkuð ítarlegt regluverk er í gildi hér á landi þegar kemur að fjarskiptaleynd og öryggi upplýsinga á almennum fjarskiptanetum. Það er svo eitt af hlutverkum Póst- og fjarskiptastofnunar að tryggja að farið sé eftir þessu regluverki.

3. Markmið um eflingu öryggisstigs

3.1 Almennt

Líkt og fram hefur komið er annað af tveimur almennum markmiðum Póst- og fjarskiptastofnunar að ná heildarsýn á stöðu öryggisstigs og öryggisvitundar sem ríkir á fjarskiptamarkaðinum. Ljóst er að stærð, staða og starfsemi fjarskiptafyrirtækja er mismunandi á íslenskum fjarskiptamarkaði. Eðli málsins samkvæmt eru þau í mismunandi stakk búinn til að byggja upp öryggisvitund og skipuleggja öryggismál sín í samræmi við alþjóðleg viðmið um bestu framkvæmd. Slík vinna er kostnaðarsöm og kallar jafnframt á nokkuð ítarlega vinnu. Aftur á mót eru öll fjarskiptafyrirtæki skuldbundin til að uppfylla þær kröfur sem að fjarskiptaregluverkið setur og ber að hlíta þeim. Þannig gerir löggjöfin ekki ráð fyrir mati stjórnvalda að mikilvægi fjarskiptafyrirtækja í þessu tilliti.

Með setningu heildstæðrar stefnu leytast stofnunin við að stuðla með sem bestum hætti að fjarskiptafélög, stór og smá, tryggi hlítni við þær kröfur sem gerðar eru til fjarskiptaleyndar og öryggis og virkni fjarskiptaneta og -þjónustu. Verður slíku markmiði best náð með því að mæta fyrirtækjum þar sem þau eru stödd á öryggisvegferð sinni og aðstoða þau við að byggja upp öryggi upplýsinga og neta í eðlilegum og raunhæfum skrefum.

Í upphafi slíkrar vinnu er nauðsynlegt fyrir stofnunina að afla upplýsinga um raunverulega stöðu öryggis fjarskiptaupplýsinga og -neta á markaðinum í dag, þ.e. að fá sýn á það hvar fjarskiptafyrirtæki sem veita almenna fjarskiptaþjónustu og/eða reka almenn fjarskiptanet standa gagnvart kröfum regluverksins er varða öryggismál. Þegar slík upplýsingaöflun hefur átt sér stað og greind mun stofnunin fá ákveðna sýn á þroskastig öryggisvitundar og stöðu öryggis upplýisnga og neta á fjarskiptamarkaðinum sem og einstakra fyrirtækja. Stofnunin mun í framhaldi af því styðja við eflingu öryggisstigs markaðarins með því að setja sértækari markmið í ákveðinum skrefum fyrir þau fyrirtæki sem eru styttra á veg komin í öryggisuppbyggingu sinni.

3.2 Mat á núverandi öryggisstigi

Svo hægt sé að styrkja með mælanlegum hætti öryggistig almennra fjarskiptaneta og almennrar fjarskiptaþjónustu hér á landi verður að ná stöðumynd af örygsstigi og öryggisvitund í dag. Hyggst stofnunin ná slíkri stöðumynd með úttekt stofnunarinnar í formi **sjálfsmats aðila á stöðu upplýsingaöryggis síns og öryggis fjarskiptaneta sinna og -þjónustu**.

Hyggst stofnunin því framkvæma sérstaka úttekt, í formi sjálfsmats aðila, á þroskastigi öryggisstigs hjá fjarskiptafyrirtækjum. Þeir aðilar sem slík sjálfsmatsúttekt mun ná til eru:

1. *fjarskiptafyrirtæki sem reka fjarskiptanetnet til veitingar almennrar fjarskiptaþjónustu og*
2. *fjarskiptafyrirtæki sem veita almenna fjarskiptaþjónustu.*

Eins og sjá má er hér um að ræða mjög víða skilgreiningu á þeim aðilum sem munu verða andlag umræddrar úttektar. Er það nauðsynlegt svo að sem best mynd fáist af stöðu öryggisstigsins á íslenskum fjarskiptamarkaði.

Framkvæmd úttektarinnar verður með þeim hætti að Póst- og fjarskipastastofnun mun senda fjarskiptafyrirtækjum spurningarlista sem hefur að geyma þrjú fyrirfram skilgreind stig

öryggisvitundar[3] sem fyrirtækin munu flokka sig í. Umrædd stig kveða á um i) lágmarksstöðu - *1. stig*, ii) góða stöðu - *2. stig* og iii) framúrskarandi stöðu – *3. stig*.

Í hvaða flokki fyrirtækið lendir, byggist á svörum þeirra sjálfra við spurningum sem settar eru fram af hálfu stofnunarinnar. Hverri spurningu fylgir ákveðið viðmið fyrir hvert stig sem fyrirtækin sjálf verða að heimfæra á stöðu sína. Umrædd stig öryggisvitundar eru skilgreind til samræmis við mynd hér til hliðar.

Lýsing á mismunandi stöðu öryggisvitundar
Stig 1 – Lágmarksstaða (basic): o Lágmarks öryggisviðmið sem gætu verið innleidd til að ná ákveðnu öryggismarkmiði. o Gögn um að lágmarksráðstafanir séu til staðar
Stig 2 – Góð staða (industry standard): o Almenn viðmið til staðar (industry standard) er varðar öryggisráðstafanir sem að ná viðkomandi markmiðum og „ad-hoc" endurskoðun á innleiðingu í kjölfar breytinga eða atvika. o Gögn um innleiðingu og viðbrögð vegna breytinga og/eða atvika.
Stig 3 – Framúrskarandi (state of the art): o Framúrskarandi öryggisviðmið og viðvarðandi eftirlit á innleiðingu, skipulögð endurskoðun á innleiðingu þar sem tekið er mið af atvikum, prófunum og æfingum, til að bæta öryggi. o Gögn um framúrskarandi innleiðingu, t.d. um skipulega úttekt á ferlum og gögn um forvirkar aðgerðir til að innleiða öryggisráðstafanir.

Spurningalistinn skiptist í mismunandi þætti sem tekur með að stjórnskipulagi upplýsingaöryggis. Innan hvers þáttar eru spurningar sem hafa mismunandi svör m.t.t. þeirra stiga sem að framan getur. Þannig getur fjarskiptafyrirætki valið um um þrjá svarmöguleika við hverri spurningu. Hver og einn svarmöguleiki hefur að geyma lýsingu í samræmi við framangreind stig/flokka og skal hvert og eitt fyrirtæki velja þann möguleika sem lýsir sem best öryggisstigi viðkomandi fyrirtækis. **Fyrirtækin svara þannig sjálf hvar þau eru stödd miðað við þær lýsingar og stöðu þeirra gagna sem þau hafa yfir að ráða.**

Þessi lýsing á mismunandi stöðu öryggisvitundar er ekki tengd hlítni við ákvæði fjarskiptalaga og afleiddra réttarheimilda með beinum hætti. Þannig á ekki að lesa þau sem lágmarksviðmið út frá kröfum laganna þótt vissulega gefi þau mynd af því hvað er lágmarksstaða öryggisvitundar. Þetta eru viðmið fyrir fyrirtæki á markaði fá heildstæða mynd af öryggisvitund innan fyrirtækis og fyrir Póst- og fjarskiptastofnun til að öðlast heildarsýn á öryggisvitund á markaði.

Öryggissjónarmið og öryggisráðstafanir eru mismunandi á milli fyrirtækja og er það alltaf á þeirra hendi og ábyrgð að byggja upp og viðhalda öryggisskipulagi sínu, framkvæma áhættumat og velja á öryggisráðstöfunum, út frá þeirra eigin þörfum og stöðu. Hins vegar er ljóst að það er eðlileg krafa að fjarskiptafyrirtæki sem eru með mikinn fjölda viðskiptavina að þau kappkosti að viðhafa framúrskarandi öryggisskipulag. Hvað varðar minni fyrirtæki og jafnvel nýja aðila á markaði má færa rök fyrir því að þau staðsetji sig á öðrum stað, a.m.k. fyrst um sinn.

Sjálfsmatsúttekt sem þessi er mjög hentug leið til að öðlast heildarmynd á öryggisvitund og stöðu öryggis á markaðinum sem og fyrir hvern og einn aðila til að öðlast góða stöðumynd af öryggisvitund fyrirtækisins. Telur Póst- og fjarskiptastofnun að slík stöðumynd sé mikilvægur liður í markvissri vinnu viðkomandi við að koma upp, viðhalda eða bæta öryggisstig

[3] Þessi úttekt byggir á fyrirmynd og leiðbeiningum frá ENISA. Technical Guideline on Security measures for Article 4 and Aricle 13a. (2014). Enisa. Sjá: https://resilience.enisa.europa.eu/article-13/guideline-on-security-measures-for-article-4-and-article-13a/TechnicalGuidelineonSecuritymeasuresforArticle4andArticle13a_version_1_0.pdf

fyrirtækisins. Póst- og fjarskiptstofnun hefur því gerð viðeigandi breytingar á afleiddum réttarheimildum, nánar tiltekið reglum nr. 1221/2007, um vernd upplýsinga á almennum fjarskiptanetum, og gert sjáfsmatsúttekt sem þess að skyldubundnum þætti í öryggisskipulagi fjarskiptafyrirtækja. Með slíkum reglubundnum úttektum næst marktæk sýn á þróun öryggisvitundar og stöðu öryggismála á fjarskiptamarkaðinum.

Líkt og áður segir mun Póst- og fjarskiptastofnun senda út spurningalista til fjarskiptafyrirtækja til framkvæmdar þessarar úttektar. Spurningalistinn sjálfur skiptist upp í mismunandi öryggisþætti. Hver þáttur hefur svo að geyma mismargar spurningar eða mismargar ráðstafanir. Hverri ráðstöfun fylgir lýsing á þeim gögnum sem þurfa að vera til staðar svo að hægt sé að segja að viðkomandi ráðstöfun sé í gildi hjá fjarskiptafyrirtækinu.

Ráðstöfunum, og gögnum sem styðja hana, er skipt í sömu stig öryggisvitundar og áður hefur verið lýst. Hver ráðstöfun hefur því þrjár lýsingar (stig). Þannig þarf hvert fjarskiptafyrirtæki að lesa viðkomandi ráðstöfun, með hvaða hætti hún er til staðar hjá fyrirtækinu og hvort til séu gögn því til stuðnings.

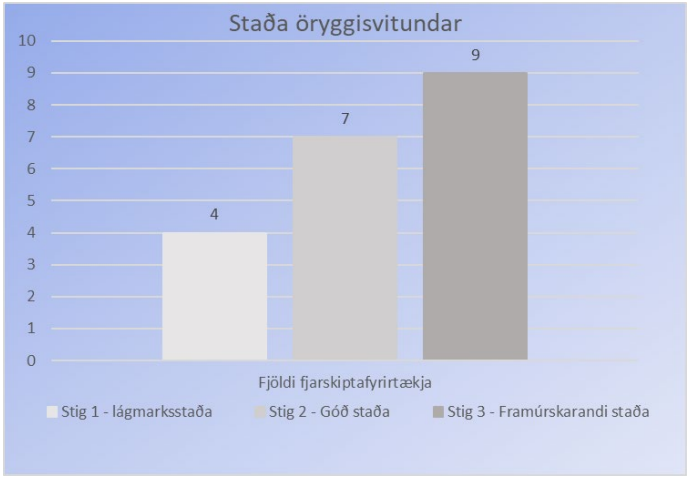
Marmið 1: Stefna um upplýsingaöryggi

	Ráðstöfun	Gögn
1	a. Gerð öryggisstefnu sem nær til öryggi fjarskiptaneta (mögulega líka upplýsinga á fjarskiptanetum). b. Starfsmenn eru meðvitaðir um tilvist stefnunnar.	○ Skrifleg öryggisstefna þar sem fram kemur: a) andlög stefnunnar, b) mikilvægar eignir, c) markmið og d) tilvísanir í viðeigandi lög ○ Lykilstarfsmenn vita af stefnunni og þekkja innihald hennar (viðtöl)
2	c. Ítarlegri upplýsingaöryggis-stefna fyrir krítískar (secondary) eignir. d. Öryggisstefna er aðgengileg og allt starfsfólk er upplýst um gildandi stefnur og hvernig þær hafa áhrif á starf þeirra. e. Endurskoðun á stefnu ef upp koma atvik.	○ Skriflegar upplýsingaöryggisstefnur fyrir krítískar eignir. ○ Starfsfólk hefur aðgang að stefnunum og hvaða áhrif það hefur að starf þeirra (viðtöl). ○ Atburðaskrár og athugasemdir nýtt til að endurskoða stefnu.
3	f. Öryggisstefna er endurskoðuð reglulega þar sem tekið er tillit til atvika, frávika, prófana og æfinga sem og atvika sem hafa haft áhrif á sambærilega aðila á markaði.	○ Upplýsingaöryggisstefnur eru uppfærðar og samþykktar af forstöðumönnum. ○ Atburðaskrár af frávikum eru samþykktar af viðeigandi starfsmönnum. ○ Endurskoðunarferli er skriflegt þar sem tekið er tillit til breytinga og atvika.

Sem dæmi um spurningu, úr þætti er varðar stjórnskipulag og áhættu-stýringu, má sjá hér til hliðar. Í þessu tilfelli er spurt um stefnu um upplýsingaöryggi.

Nauðsynlegt er að taka fram að til að falla í flokk tvö þarf fyrirtæki jafnframt að uppfylla ráðstafanir og gögn í flokki eitt. Hið sama á við flokk þrjú. Þannig eru það einungis fjarskiptafyrirtæki sem að uppfylla alla flokkanna sem geta staðsett sig í flokki þrjú.

Að fengnum svörum frá fjarskiptafyrirtækjum mun Póst- og fjarskiptastofnun vinna niðurstöður og þannig öðlast yfirsýn yfir það hvar öryggisvitund á fjarskipta-markaðinum liggur. Þetta skapar stofnuninni grundvöll til að vinna með þeim aðilum sem sjá færi á að bæta öryggisvitund sína og auka öryggi fjarskiptaupplýsinga og virkni fjarskiptaneta sinna. Allar niðurstöður yrðu háðar trúnaði þannig yrði birting niðurstaðna úr úttekt sem þessari með þeim hætti að ekki væri hægt að lesa út hvernig einstök fyrirtæki telja öryggisvitund sína vera.



3.3 Efling öryggisstigs

Á grundvelli framangreindrar niðurstöðu mun Póst- og fjarskiptastofnun geta hvatt einstök fjarskiptafyrirtæki til að efla öryggisstig sitt og öryggisvitund með gerð sértækari markmiða hvað það varðar.

Póst- og fjarskiptastofnun áréttar mikilvægi góðs samstarfs við fjarskiptafélög og mun stofnunin leitast við að mæta fjarskiptafyrirtækjum með sanngjörnum hætti eftir stærð þeirra og umfangi þjónustu, þótt öll eru þau þó í raun undir sama hatt kominn þegar kemur að hlítni við kröfur fjarskiptalaga. Þannig munu þau fjarskiptafyrirtæki sem eru styttra á veg komin með uppbyggingu öryggisskipulags síns fá tækifæri til þess að fara í viðeigandi vinnu til úrbóta áður en stofnunin fer í ítarlegri greiningu eða sértækari úttektir á því hvort að viðkomandi uppfylli kröfur fjarskiptalaga og afleiddra réttarheimilda.

Það er því markmið stofnunarinnar að efla öryggisstig á fjarskiptamarkaðinum í samvinnu við aðila og telur stofnunin að framkvæmd eftirlits með þessum hætti sé færsælast til árangurs.

4. Markmið um virkni og þanþol fjarskiptainnviða

4.1 Almennt

Virkni fjarskiptainnviða og þanþol þeirra er grundvallarforsenda órofinnar fjarskiptaþjónustu. Það er því mikilvægt að virkni þeirra sé tryggð og þanþol þeirra skoðað og metið með sem bestum og nákvæmustum hætti. Fjarskiptafyrirtækin hafa þá skyldu, hvert fyrir sig, að tryggja virkni neta sinna og samfellu þjónustu. Hins vegar er ljóst að það er ekki hlutverk þeirra að hafa yfirsýn yfir virkni fjarskiptaneta almennt hér á landi. Slík yfirsýn verður að vera á hendi stjórnvalda enda miklir þjóðhagslegir hagsmunir fólgnir í því að fjarskiptaþjónusta og fjarskiptasambönd hér á landi séu trygg. Slík yfirsýn verður þó ekki fengin nema með náinni samvinnu við rekstraraðila netanna og þjónustunnar. Það er því stefna Póst- og fjarskiptastofnunar að koma slíkri samvinnu á fót og ná heildstæðri mynd af fjarskiptainnviðum hér á landi og þeirri áhættu sem að þeim staðar.

Að fenginni slíkri heildarmynd er hægt að afmarka með betri hætti hvar áherslur á öryggi ættu að liggja og greina sértækari markmið um eflingu á virkni og þanþoli þeirra. Slíkt yrði t.a.m. sett fram í úttektaráætlun.

4.2 Áhættumat fjarskiptainnviða

Að tryggja heildstæði og virkni almennra fjarskiptaneta hér á landi er mikil áskorun fyrir alla sem koma að rekstri þeirra og veitingu fjarskiptaþjónustu. Fjarskiptaþjónustan er mismunandi, allt frá hefðbundnum talsíma yfir í háhraða farnetsþjónustu. Fjarskiptanetin eru með sama hætti mjög mismunandi, byggð upp með mismunandi hætti (farnet og fastanet) og af mismunandi aðilum. Þau hafa mismunandi hlutverk í virðiskeðju fjarskiptanna, allt frá sæstrengjum og stofnstrengjum til einstakra farnetssenda. Allt eru þetta fjarskiptainnviðir sem eru nauðsynlegir til veitingar fjarskiptaþjónustu í nútímasamfélagi. Að mati Póst- og fjarskiptastofnunar skortir í dag ákveðna yfirsýn yfir öryggi og heildstæði fjarskiptainnviða, hvar stærstu áhættur liggja og möguleika fyrirtækjanna til að standast áhættur og bregðast við þeim.

Líkt og fjallað hefur verið um þá ber fjarskiptafyrirtækjum að framkvæma áhættumat, setja niður skriflegar öryggisráðstafanir á grundvelli þess sem og að setja sér neyðaráætlun um samfelldan og órofinn rekstur. Þetta ber hverju fjarskiptafyrirtæki að gera. Stofnunin fer með eftirlit hvað þetta varðar og hefur á undanförnum árum staðið að mismunandi úttektum á einstökum þáttum fjarskiptainnviða, svo sem mikilvægum tækjarýmum Mílu, hýsingarrýma á landtökustöðum FARICE-1 og DANICE sem og farið hefur verið yfir varaafl farnetssenda á náttúruvásvæðum við Kötlu og Öræfajökul.

Við undirbúning og framkvæmd þessara úttekta og í samtölum við hagmsmunaaðila hefur Póst- og fjarskiptastofnun orðið þess áskynja að aðilar telja að nálgast mætti hlutina með heildstæðari hætti. Póst- og fjarskiptastofnun tekur undir þessi sjónarmið og setur sér því það almenna markmið í þessari stefnu að öðlast heildstæðari mynd af stöðu og þanþoli fjarskiptainnviða hér á landi. Stofnunin hyggst því framkvæma áhættumat á ákveðnum mikilvægum fjarskiptainnviðum sambærilegum þeim sem framkvæmdar hafa verið af systureftirlitsstofnunum á Norðurlöndunum. Svo vel takist til þarf að stofnunin að eiga náið og gott samstarf við rekstraraðila netanna og veitendur fjarskiptaþjónustu. Er það von stofnunarinnar að slíkt náist.

Með framkvæmd mats sem þessa getur stofnunin öðlast yfirsýn yfir stöðu, samvirkni og stærstu áhættu sem steðjar að fjarskiptainnviðum. Er ætlunin að áhættumatið dragi fram heildarmynd af áhættu sem stafar að innviðum fjarskipta og geta valdið alvarlegum truflunum og rofi á fjarskiptum og getu fjarskiptafyrirtækja til að bregðast við henni. Niðurstöður matsins, sem

aðilar hafa unnið sameiginlega að, munu jafnframt veita stofnuninni leiðarljós í forgangsröðun við gerð úttektaráætlunar á fjarskiptainnviðum. Verkefni sem þetta er umfangsmikið og kallar á mikla undirbúningsvinnu, faglega þekkingu og góða samvinnu við alla aðila á markaði.

Ljóst er að mat á öryggi, virkni og þanþoli fjarskiptainnviða er verkefni sem þarf stöðugt að vinna að og endurmeta. Er það jafnframt ætlun stonfunarinnar að áhættugreining sem þessi verði uppfærð með reglulegu millibili og í samstarfi við aðila á markaði.

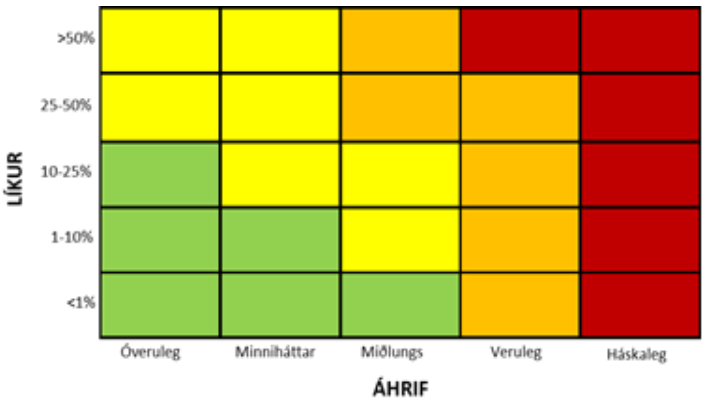
Ljóst er að afmökrkun á umfangi og fjarskiptainnviðum skiptir sköpun svo sem raunsæasta niðurstaða fáist. Áhættumatið mun því afmarkast við **áhættu sem getur valdið alvarlegum truflunum á virkni fjarskiptaneta og/eða rofi á veitingu fjarskiptaþjónustu, annað hvort á stórum landssvæðum, og/eða varðar mikinn fjölda notenda.**

Eins verður einnig metið hvort **truflanir og/eða rof geti orðið til þess að lífi notenda hérlendis sé ógnað eða verulegar efnahagslegar afleiðingar hljótist af.**

Póst- og fjarskiptastofnun hefur þegar hafið undirbúningsvinnu við umrædda áhættugreiningu. Sýnir sú undirbúningsvinna að mikilvægt er að flokka fjarskiptainnviði eftir tegund þeirra og mikilvægi sem og skilgreina ógnir og veikleika sem geta valdið, eða talið er að geti valdið rofi, og/eða alvarlegum truflunum í fjarskiptanetum.

Við framkvæmd áhættumatsins verður unnið eftir viðurkenndri og þekktri aðferðarfræði með utanaðkomandi sérfræðingum, sérfræðingum stofnunarinnar sem og hagsmunaaðilum. Verður leytast við að greina eðlislæga áhættu fjarskiptainnviða sem og að ákveðið getumat verður framkvæmt. Mat á viðbragðsgetu fjarskiptainnviða þarf að skoða m.t.t. högunar, varnarbúnaðar, viðbragðsaðila og tæknilegra þátta eins og þanþols og umfremdir (e. capacity). Við framkvæmd áhættumats verður tekið tillit til þess hvaða stýringar eru til staðar (núverandi áhætta (e. current risk)) og hvort að eftirstæð áhætta (e. residual risk) sé fyrir hendi. Framkvæmt verður áhættuskor fyrir skilgreindar ógnir og áhættu en stofnuin mun viðhafa samráð við aðila við frekari útfærslu á aðferðafræði við mat áhrifa áhættu.

Við framkvæmd áhættumatsins verður notast við aðferðafræði sem byggir á huglægu mati og 10x10 áhættuskorun fyrir eðlislæga áhættu sem og eftirstæða áhættu. Þannig verður sú áhætta sem skorar hátt metin sérstaklega m.t.t. ráðstafan og skoruð á ný. Fari svo að áhætta sé umfram æskileg viðmið fyrir áhættu er slík áhætta flokkuð sérstaklega sem eftirstæð áhætta. Mynd hér til hliðar sýnir útfærslu af framsetningu á niðurstöðum sem byggir á slíkri aðferðafræði.[4]



[4] Myndin sýnir 5x5 skorun en ætlunin er áhættugreiningin byggi á 10x10 áhættuskorun.

Líkt og áður segir mun Póst- og fjarskiptastofnun nýta sér niðurstöður þessa umfangsmikl mats til að ákveða forgagnsröðun verkefna sinna. Slík forgangsröðun verður grundvöllur úttektaráætlunar stofnunarinnar sem felur í sér sértækari markmið stofnunarinnar um eflingu á virkni fjarskiptainnviða og þanþols þeirra.

Þá mun ítarleg grunnvinna sem þessi nýtast til framkvæmdar reglubundins endurmats. Með slíku reglubundnu endurmati telur Póst- og fjarskiptastofnun að góð og marktæk heildarsýn náist yfir þróun stærstu eðlislægu áhættu, virkni og þanþol mikilvægra fjarskiptainnviða hér á landi.

5. Úttektaráætlun - Sértæk markmið um þanþol og virkni

5.1 Almennt

Póst- og fjarskiptastofnun hefur á undanförnum árum framkvæmt úttektir á mjög afmörkuðum hlutum einstakra fjarskiptainnviða. Hefur stofnunin við framkvæmd þeirra notast við þekkt úttektarform, svo sem skrifborðsúttektir og vettvangsskoðanir. Hefur stofnunin byggt upp aðferðarfræði við úttektir sem byggjast á þekktum og viðurkendum aðferðum.

Hin sértæku markmið Póst- og fjarskiptastofnunar varðandi virkni og þanþol fjarskiptainnviða felast í markvissari eftirlitsstarfsemi sem byggir á niðurstöðu áðurnefnds áhættumats. En með því munu skapast forsendur fyrir skýrari forgangsröðun við framkvæmd eftirlits en fram til þessa. Stofnunin telur því mikilvægt að samhliða slíkri forgangsröðun verði sett fram skýr aðferðarfræði þeirra úttektarforma sem stofnunin hyggst nota við framkvæmd eftirlits síns.

Það er ljóst að til eru mismunandi leiðir við framkvæmd eftirlits af þessu tagi. Stofnunin mun áfram byggja vinnu sína á þekktum og viðurkenndum aðferðum og mun líta til leiðbeininga frá Netöryggisstofnun Evrópu (ENISA). Póst- og fjarskiptastofnun hefur jafnframt í hyggju að setja sér verklagsreglur um aðferðarfræði og framkvæmd úttekta. Með setningu slíkra verklagsreglna mun fullt gagnsæi ríkja um þær tegundir úttekta sem stofnunin hyggst nýta, aðferðarfræði þeirra og viðmið stofnunarinnar. Það er einnig markmið stofnunarinnar að með slíkum reglum muni verklag úttekta verða staðlaðra og þekktara á meðal fjarskiptafyrirtækja. Mun það auka traust og samvinnu milli stofnunarinnar og fjarskiptafyrirtækja.

Verður nú varpað ljósi á þá aðferðarfræði sem úttektaráætlun stofnunarinnar mun byggja á sem og þær verklagsreglur sem stofnunin hyggst setja sér við framkvæmd úttekta. Verður fyrst fjallað um ákveðnar tegundir matsaðferða og síðar um mismunandi framkvæmdaraðila úttekta.

5.2 Aðferðafræði úttekta PFS

Við framkvæmd úttekta er hægt að styðjast við mismunandi matsaðferðir. Sem dæmi má nefna mat á skjölum og gögnum (skrifborðsúttektir) þar sem t.d. öryggisstefnur eru yfirfarnar. Þá er hægt að meta stöðu aðila í gegnum viðtöl við starfsmenn og/eða stjórnendur fyrirtækja. Eins er hægt að framkvæma vettvangsskoðun og athuga stöðu aðila með beinum hætti. Framkvæmd úttektar getur stuðst við eina tegund matsaðferðar, tvær eða fleiri, allt eftir umfangi úttektar og tegundar úttektarandlags.

Matsaðferðir:

Mat í formi yfirferðar á gögnum (skrifborðsúttekt)

Almennt eru skrifborsúttektir, þar sem farið er yfir skjöl og gögn frá aðilum, nauðsynlegur hluti allra úttekta. Gögn frá aðilum geta verið öryggisstefnur, áhættumat og valdar öryggisráðsstafanir, neyðaráætlanir, einstaka hlutverk aðila og ábyrgðadreifing, verklagsreglur og verklýsingar, lýsingar á hönnun og uppbyggingu kerfa sem og innri prófanir og niðurstöður þeirra.

Mat í formi viðtala

Mat í formi viðtala er vel þekkt. Getur það verið framkvæmt hvort sem er sjálfstætt eða til viðbótar við yfirferð gagna með skrifborðsúttekt en hægt er hægt að afla mikilla upplýsinga í gegnum viðtöl við starfsmenn viðkomandi aðila. Fjöldi viðmælenda getur verið mismunandi eftir stærð fjarskiptafyrirtækis þar sem hjá smærri aðilum getur reynst nægjanlegt að tala við fáa aðila sem hafa tiltölulega mikla og víðtæka ábyrgð innan fyrirtækisins. Hjá stærri aðilum getur verið nauðsynlegt að ræða við fleirri þar sem ábyrgðin er mögulega dreifðari.

Mat í formi beinnar athugunar
Mat í formi beinnar úttektar eða athugunar á kerfi eða öðrum þætti fjarskiptainnviðar er ítarlegasta tegund mats. Með þessu eru t.a.m. kerfi athuguð og/eða prófuð með beinum hætti. Hér er t.d. um að ræða hefðbundnar vettvangsathuganir þar sem að starfsmenn stofnunarinnar, eða fulltrúar á hennar vegum, hafa varið á viðkomandi stað og athugað hvort t.a.m. viðkomandi öryggisráðstöfun sé til staðar. Hérna getur þó jafnframt verið um að ræða úttektir sem framkvæmdar eru af innri eða ytri aðila.

Framkvæmdaaðilar úttekta:

Það getur einnig verið mismunandi hvaða aðilar framkvæma úttekt, hvort sem hún byggist á einni eða fleiri matsaðferðum. Þannig getur aðili sjálfur gefið skýrslu eða upplýsingar um stöðu mála eftir sjálfsmat, innri eftirlitsaðiliar geta framkvæmt úttekt, sem og ytri úttektaraðilar og þar með talið eftirlitsstofnanir.

Sjálfsmat aðila
Með sjálfsmati þá meta aðilar sjálfir stöðu sína gagnvart fyrirfram ákveðnum spurningum og mælikvörðum. Þessari tegund úttektaraðferðar er ætlað að veita eftirlitsaðila ákveðna almennar upplýsingar um stöðu aðila á markaði. Kostir þessarar aðferðarfærði er að hún er tiltölulega ódýr fyrir viðkomani aðila.

Í sjálfsmatsúttekt er jafnframt hægt að bæta við skilyrðum um að svör aðila í sjálfsmati séu studd skriflegum gögnum, t.a.m. að svörunum fylgi úttektarstefan, áhættumat o.s.frv. Þá er einnig hægt að fylgja sjálfsmatinu eftir með viðtölum við aðila.

Skoðun innan félags
Ein tegund úttektar er framkvæmd innri endurskoðunar. Hér er um að ræða yfirferð starfsmanns eða deildar viðkomandi félags, sem framkvæmdi úttektir á ákveðnum kerfum, hluta kerfa félagsins, rýma þess eða áætlana. Það sem þessi tegund úttektar hefur framyfir sjálfsmatsaðferðina er að í flestum tilvikum er viðkomandi innri úttektaraðili sjálfstæðari í verkum sínum, þ.e. við að framkvæma úttektina sjálfa. Kostir þessarar tegundar úttektar, t.d. samanborði við ytri endurskoðun, er að úttektaraðilinn þekkir félagið mun betur og skilur með mun dýpri hætti uppbyggingu þeirra kerfa, neta og rýma sem að félagið nýtir í starfsemi sinni.

Eftirlitsaðili getur hér hvort tveggja óskað skjalfestingar á að innri endurskoðun hafi farið fram, fengið niðurstöðu hennar skjalfesta og/eða beitt viðtalsaðferð.

Skoðun ytri aðila
Framkvæmd ytri endurskoðunar felur í sér að ytri aðili framkvæmdir úttekt á viðkomandi aðila, að hans frumkvæði. Hér er um að ræða sjálfstæðan aðila sem er í raun óháður félaginu sjálfu sem og eftirlitsaðila. Þessi aðili þekkir síður til hvernig einstaka félag byggir upp þjónustu sína og kerfi. Þetta getur leitt til þess að kostnaður getur orðið hærri en ef að innri endurskoðun er framkvæmd enda þarf viðkomandi félag að gefa úttektaraðila tíma og, oft á tíðum, nákvæmar upplýsingar um uppbyggingu neta, einstök kerfi og stillingar kerfa. Hins vegar getur þetta átt betur við minni fyrirtæki sem ekki hafa svigrúm til að hafa virka innri endurskoðun.

Úttektir Póst- og fjarskiptastofnunar
Hér er um að ræða úttektir sem ýmist eru framkvæmdar af Póst- og fjarskiptastofnun sjálfri eða ytri aðilum á hennar vegum.

Hér getur verið um að ræða almennar úttektir t.d. hefðbundar skrifborsðúttektir þar sem stofnunin kallar eftir viðeigandi gögnum, t.d. öryggisstefnu félagsins, áhættumati þess, viðbragðsáætlun o.s.frv., vettvangsskoðanir stofnunarinnar á einstökum tækjarýmum eða úttekt á einstaka kerfum eða hluta kerfa félags.

Hér geta einnig komið til skoðunar sértækari skoðanir, t.d. á öryggisatvikum sem upp geta komið. Þá getur stofnunin ýmist nýtt þekkingu starfsfólks síns eða kallað að ytri sérfræðinga til að fara yfir viðkomandi atvik.

Vettvangsskoðun vottaðs aðila
Þessi tegund skoðunar felur í sér úttekt vottaðs ytri aðila á hlítni fyrirtækis gagnvart ákveðnum staðili, t.a.m. ISO 27001. Hafi fyrirtæki gengið í gegnum vottunarferli sem þetta og staðist vottum samkvæmt staðli á tilteknum hluta starfsemi sinnar eða hluta kerfa verður að skoða umfang slíkrar vottunar í samhengi við kerfi og þjónustu viðkomandi. Þess ber að geta að slík vottun kemur ekki sjálfkrafa í stað eftirlits Póst- og fjarskiptastofnunar.

5.3 Verklagsreglur Póst- og fjarskiptastofnunar

Pót- og fjarskiptastofnun hefur á undanförnum árum framkvæmt mismunandi úttektir á hvort tveggja raunlægu öryggi tækjarýma hjá fjarskiptafélögum, meðferð og eyðingu á fjarskiptaumferðarupplýsingum sem og á stöðu varaafls á náttúruvásvæðum. Hefur í þessari vinnu byggst upp ákveðin aðferðarfræði sem stofnun hefur tileinkað sér.

Til að auka gagnsæi í stjórnsýslu stofnunarinnar við framkvæmd eftirlits á þessu sviði hyggst stofnunin setja sér verklagsreglur um framkvæmd úttekta. Í þeim verklagsreglum verður sett fram aðferðarfærði sem stofnunin mun fylgja í þeim úttektarverkefnum sem hún hyggst fara í.

Umræddar verklagsreglur munu í grunninn byggja á þekktri aðferðarfræði við úttektir á grundvelli staðla. Aftur á móti er ljóst að Póst- og fjarskiptastofnun, sem eftirlitsstjórnvald, hefur ekki sama hlutverk og sjálfstæður úttektaraðili vegna t.a.m. vottunar. Stofunin þarf að lokum að heimfæra skipulag öryggissins yfir á kröfur laganna í formi stjórnvaldsákvörðunar.

Þannig hefur stofnunin, framkvæmd úttekta sinna fram til þessa, tekið stjórnvaldsákvarðanir um hlítingu. Hefur í mörgum tilfellum skapast ákveðin sátt um þessa aðferðarfræði. Munu verklagsreglurnar endurspegla þá framkvæmd sem verið hefur sem og framangreindar aðferðar, að því marki sem mögulegt er. Þá munu þær fara í sérstakt samráðsferli þegar þar að kemur.

6. 5G fjarskiptanet

Kröfur fjarskiptalaga og afleiddra réttarheimilda gilda óháð þeirri tækni og þjónustu sem að fjarskiptafélög nota. Ekki eru því sérstakar kröfur í íslenskum lögum sem gilda um öryggi 5G fjarskiptaneta umfram almennar kröfur laganna. Hins vegar er ljóst að mikilvægi fjarskiptaneta fer vaxandi og mun 5G tækni fjarskiptaþjónustu gera fjarskiptanetin enn mikilvægari í efnahagslegu tilliti og þegar litið er til samkeppnishæfni þjóða. Gríðarlegt magn gagna og tengdra hluta (IoT) ásamt þeirra möguleika sem að þessi tækni og net bjóða uppá t.d. í iðnstýrignum, framleiðslu, heilbrigðisþjónustu o.fl. gera þessi net að grundvallarstoð þjóðfélaga á næstu árum. Það er því ekki óeðlilegt að öryggi þeirra og þanþol sé skoðað sérstaklega og metið.

Evrópusambandið hefur á undanförunum misserum gefið út lagagerðir varðandi öryggi 5G neta og þeirrar þjónustu sem að veitt er yfir slík net. Þar má í fyrsta lagi nefna tilmæli framkvæmdastjórnarinnar frá því í mars sl. varðandi öryggi 5G neta.[5] Tilmælin fela í sér ákveðið ferli til að meta og mæta mögulegum ógnum sem stafað geta að 5G netum. Kveða þau á um að aðildarríki skuli framkvæma landsbundið áhættumat varðandi öryggi 5G netanna og endurskoða þær ráðstafanir sem að þau geta gripið til varðandi það. Þetta landsbundna áhættumat hafa þau hafa nú þegar framkvæmt og sent framkvæmdastjórn Evrópusambandsins og ENISA. Eins hefur samstarfshópur NIS-tilskipunarinnar[6] (e. Cooperation Group) gefið út skýrslu varðandi samhæft evrópskt áhættumat 5G neta.[7] Þá hefur ENISA jafnframt birt ítarlega skýrslu um ógnarmynd (e. threat landscape) 5G kerfa.[8] Umræddar skýrslur og áhættumöt eru í samræmi við þær aðgerðr sem að framangreind tilmæli kveða á um. Þá hefur samstarfshópuinn birta skýrslu um mögulegar mótvægisaðgerðir sem aðildarríki geti gripið til svo að auka megi öryggi netanna.[9] Umrædd tilmæli hafa ekki verið tekin upp í EES-samningin og eru íslensk stjórnvöld því ekki skuldbundin til að innleiða þau í íslenskan rétt. Aftur á móti telur Póst- og fjarskiptastofnun eðlilegt og mikilvægt að fylgjast með þróun og útkomu þessara vinnu og bregðast við ef að stofnunin telur þörf fyrir slíkt. Ísland fylgir mörgum þeim gerðum sem komið hafa frá Evrópu þegar kemur að öryggi fjarskiptaneta og upplýsingainnviða. Má þar m.a. nefna eldri tilskipanir á sviði persónuverndar, nýrrar reglugerðar á sviði persónuverndar, löggjafar á sviði fjarskipta og nú síðast, öryggi net- og upplýsingakerfa mikilvægra innviða. Þessi þróun mun halda áfram.

Í öðru lagi má nefna nýsamþykkta reglugerð Evrópusambandsins á sviði netöryggis, þ.e. reglugerð 2019/881 frá 17. apríl sl., um ENISA og vottunarferli netörygis á sviði upplýsinga-

---

[5] Commission Recommendation of 26 March 2018. Cybersecurity of 5G networks. Sjá: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=EN

[6] Directive (EU) 2016/1148 of the Europena Parliament and the Council of 6 July 2016 concerning measures for high common level of security of networks and information systems across the Union. Sjá: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[7] Skýrsla samstarfshóps NIS-tilskipunarinnar. EU coordinated risk assessment of the cybersecurity of 5G networks. 9. október 2019: Sjá: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

[8] ENISA Threat Landscape for 5G Networks. 21. nóvember 2019. Sjá: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[9] Skýrsla samstarfshóps NIS-tilskipunarinnar. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. 01/2020. Sjá: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

og fjarskiptatækni.[10] Í þessari reglugerð er ENISA gefið varanlegt hlutverk sem Netöryggisstofnun Evrópu sem og að sett er á stofn samevrópskt vottunarferli fyrir búnað fyrir upplýsinga- og fjarskiptatækni, slíkar þjónustu og ferla.[11] Umrætt ferli gerir ráð fyrir samvinnu milli framkvæmdastjórnarinnar, ENISA og ákveðinna sérfræðihópa sem settir eru á stofn með reglugerðinni og annarra aðila. Þetta ferli er á byrjunarreit í dag. Hins vegar vinnur EFTA skrifstofan að því að innleiða viðkomandi reglugerð inn í EES-samninginn og eru því líkur á því að hún muni vera innleidd í íslenskan rétt. Póst- og fjarskiptastofnun mun að sjálfsögðu fylgjast með framvindu mála hvað þetta varðar.

[10] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification an repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Sjá: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[11] Information and Communi technologies (ICT products, ICT services and ICT processes).

7. Samantekt

Í skjali þessu hefur Póst- og fjarskiptastofnun sett fram sýn sína og áætlanir er varðar öryggi og virkni fjarskiptainnviða. Í upphafi skjalsins var hlutverk stofnunarinnar kynnt sem og fjallað var um kröfur fjarskiptalaga, nr. 81/2003 og afleiddra réttarheimilda hvað varðar öryggi upplýsinga á almennum fjarskiptanetum og virkni almennra fjarskiptaneta. Ljóst er að von er á nýrri heildarlöggjöf á sviði fjarskipta á næstu misserum þar sem gera má ráð fyrir ákveðnum breytingum.

Þá hefur verið sett fram tvíþætt markmið stofnunarinnar, þ.e. í fyrsta lagi að kanna stöður öryggisstigs og öryggisvitundar heilt yfir allan markaðinn og, í öðru lagi, að öðlast yfirsýn yfir með gerð ítarlegrar áhættugreiningar. Bæði þessi markmið fela í sér ákveðin undirmarkmið svo sem við að hvetja til eflingar öryggisvitundar og tryggja með sem bestum hætti virkni almennra fjarskiptaneta. Það síðarnefnda felur í sér ákveðna úttektaráætlun stofnunarinnar og setningu verklagsreglna þar um.

Að lokum var fjallað um aðgerðir á vegum Evrópusambandsins varðandi öryggi 5G neta. Póst- og fjarskiptastofnun mun fylgjast með þróun mála á Evrópuvísu hvað varðar öryggi 5G neta og þjónustu sem kann að byggja á þeirri tækni.

Að mati stofnunarinnar er mikilvægt sjónarmið hagsmunaaðila á þessa sýn stofnunarinnar komi fram. Því eru þessi stefnudrög sett í opið samráð. Stofnunin áréttar sem fram hefur komið í skjali þessu að markmið stofnunarinnar hlýtur að fara saman með markmiðum markaðsaðila á þessu sviði, þ.e. að efla öryggisvitund hjá fjarskiptafyrirtækjum og að tryggja með sem bestum hætti öryggi upplýsinga og tryggja með sem bestum hætti virkni og þanþol fjarskiptainnviðinna þannig að til þjónusturofs komi ekki. Óskar stofnunin því eftir farsælu samstarfi við fjarskiptafyrirtæki til að ná þessum markmiðum.

Póst- og fjarskiptastofnun óskar eftir sjónarmiðum, athugasemdum og tillögum frá hagsmunaaðilum hvað varðar efni þessara stefnudraga. Er frestur veittur til föstudagsins 20. desember nk.

PÓST- OG FJARSKIPTASTOFNUN

2020