NET- OG UPPLÝSINGAÖRYGGI

SKÝRSLA STARFSHÓPS SAMGÖNGURÁÐHERRA
UM ÖRYGGI FJARSKIPTA O.FL.

Samgönguráðuneytið
Reykjavík, nóvember 2006
www.samgonguraduneyti.is

Efnisyfirlit

Formáli

Í maí 2005 skipaði samgönguráðherra starfshóp um öryggi fjarskipta. Starfshópnum var m.a. falið að vinna tillögur á því sviði í samræmi við stefnu ríkisstjórnarinnar um upplýsingasamfélagið, *Auðlindir í allra þágu*, og að hafa til hliðsjónar markmið fjarskiptaáætlunar fyrir árin 2005 – 2010.

Markmið starfsins var að einfalda stjórnsýslu og efla öryggi við notkun upplýsinga- og fjarskiptatækni sem og þjónustu við borgarana.
Verkefni nefndarinnar var m.a. að skoða:

- þær ógnir sem steðja að fjarskiptum og upplýsingatækni m.t.t. rafrænna hryðjuverka og annarra hliðstæðra verka,
- tilfelli þar sem borgararnir verða fyrir áreiti vegna óumbeðins markpósts eða annarra sambærilegra atvika,
- hlutverk stjórnvalda á þessu sviði og eftir atvikum skilgreina það,
- ákvæði laga er varða hlutverk stjórnvalda og úrræði til þess að framfylgja stjórnvaldsákvörðunum.

Auk þess var starfshópnum falið að skila útfærðum tillögum um verkaskiptingu stofnana ríkisins og koma með ábendingar varðandi þörf á endurskoðun laga vegna samþættingar upplýsingatækni, fjarskipta og fjölmiðlunar.

Í starfshópnum sátu eftirtaldir aðilar Árni Albertsson f.h. dóms- og kirkjumálaráðuneytis, Jóhann Gunnarsson f.h. fjármálaráðuneytis, Guðbjörg Sigurðardóttir frá forsætisráðuneyti, Davíð Davíðsson frá Hagstofu Íslands, Sigfús Ingi Sigfússon frá iðnaðar- og viðskiptaráðuneyti, Jón Vilberg Guðjónsson frá menntamálaráðuneyti, Karl Alvarsson frá samgönguráðuneyti, Björn Geirsson frá Persónuvernd og Hörður Halldórsson frá Póst- og fjarskiptastofnun. Fulltrúi Hagstofunnar hvarf fljótlega úr hópnum við flutning Þjóðskrár frá Hagstofunni til dóms- og kirkjumálaráðuneytis. Þá létu fulltrúar Póst- og fjarskiptastofnunar og Persónuverndar af störfum án þess að nýir væru skipaðir í þeirra stað. Fulltrúi síðarnefndu stofnunarinnar sat fundi og starfaði með hópnum til loka starfsins sem starfsmaður Póst- og fjarskiptastofnunar. Starfshópurinn hélt um 30 fundi, þ.m.t. kynningar og fór í heimsóknir til fjarskiptafyrirtækja og markaðsaðila, sem voru mjög gagnlegir og upplýsandi um stöðu þessara mála hér á landi.

Þær tillögur, sem hér koma fram eru fyrstu skref stjórnvalda til samræmingar á sviði net- og upplýsingaöryggis. Ekki má þó gleyma því að fyrirtæki í fjarskiptum, net- og öryggisþjónustu hafa unnið gott verk án verulegra afskipta stjórnvalda, þó að víða sé að finna ákvæði í lögum um efnið. Ljóst er að ríkin í kringum okkur eru flest komin mun lengra og til þeirra höfum við m.a. horft í þessu starfi, enda má margt af þeirra reynslu læra. Þá hefur Evrópusambandið og ýmsar alþjóðlegar stofnanir verið með stefnumótun um þessi mál. Reynslan erlendis sýnir að öryggi á þessu sviði snýst ekki bara um reglur og tækni heldur að miklu leyti um hugarfar.

Reykjavík 29. nóvember 2006

f.h. starfshópsins

Karl Alvarsson, formaður

Meginniðurstöður og tillögur

Almenn markmið / tillögur

I. Unnið verði að því með markvissum hætti að þróa öryggisvitund í samfélaginu.

1. Lögð verði áhersla á aukna fræðslu og miðlun upplýsinga til almennings um net- og upplýsingaöryggi. (3.3)
   Ábyrgð: Menntamálaráðuneyti, samgönguráðuneyti, Póst- og fjarskiptastofnun, fjarskiptafyrirtæki, félagasamtök.

2. Fjarskiptafyrirtæki, þ.m.t. netþjónustuaðilar, eftirlitsaðilar, stjórnvöld og félagasamtök, samræmi upplýsingagjöf til almennings um net- og upplýsingaöryggi. Þessir aðilar vinni saman að gerð leiðbeiningarefnis til dreifingar til almennings og í skólum. Póst- og fjarskiptastofnun hafi frumkvæði að samstarfi og samræmi hlutverk stjórnvalda. (3.3)
   Ábyrgð: Póst- og fjarskiptastofnun.

3. Komið verði upp vefsíðu með leiðbeiningum varðandi öll erindi eða kvartanir á sviði net- og upplýsingaöryggis burtséð frá því hver ber ábyrgð á úrlausnarefninu (3.3)
   Ábyrgð: Persónuvernd, Póst- og fjarskiptastofnun og Ríkislögreglustjóri komi sér saman um framkvæmd þessa þáttar.

4. Opinberar stofnanir hugi að netnotkun starfsmanna og umgengni um tölvupóst. Hafa má til hliðsjónar vinnureglur Persónuverndar um netnotkun starfsmanna. (3.2)
   Ábyrgð: Allar opinberar stofnanir.

5. Þjónustuaðilar og samtök, sem starfa á sviði internetþjónustu hvetji til notkunar varnarbúnaðar og leggi áherslu á þennan þátt í kynningarefni. (3.11.2)
   Ábyrgð: Netþjónustuaðilar, félagasamtök.

II. Lögð verði áhersla á að byggja upp traust á upplýsingasamfélaginu öryggi innviða þess og samkeppnishæfni..

6. Neytendum verði boðið upp á þjónustu sem takmarki aðgang að ólögmætu eða ósiðlegu efni frá netþjónustuaðilum. (3.3)
   Ábyrgð: Netþjónustuaðilar.

7. Unnið verði að því að takmarka aðgang að ólögmætu eða ósiðlegu efni í almenningsbókasöfnum, grunn- og framhaldsskólum. (3.3)
   Ábyrgð: Menntamálaráðuneyti, sveitarfélög, grunnskólar, bókasöfn, framhaldsskólar.

8. Seljendum tækja, búnaðar og þjónustu verði skylt að upplýsa kaupendur eða notendur þjónustu um örugga notkun, um helstu veikleika og hvernig best sé að varast þá og geri efnið aðgengilegt, t.d. á heimasíðum sínum. Jafnframt verði þeim gert skylt að afhenda búnað þannig stilltan að hann sé varinn og sú skylda hvíli á þeim að leggja neytendum til reglulega uppfærslu á nauðsynlegum vörnum. (3.3.1)
   Ábyrgð: Póst- og fjarskiptastofnun.

9. Netþjónustuaðilar taki upp skýr ákvæði í skilmála sína sem heimili þeim síun ruslpósts að fengnu samþykki kaupenda. (3.5)
   Ábyrgð: Netþjónustuaðilar.

10. Útbreiðsla rafrænna skilríkja og gerð dreifilyklaskipulags fyrir allt landið verði forgangsmál stjórnvalda, og þau hafi frumkvæði að því að taka upp rafræn skilríki. (3.6)
    Ábyrgð: Fjármálaráðuneyti.

11. Settar verði leiðbeinandi reglur um notkun rafrænna skilríkja hjá ráðuneytum og ríkisstofnunum þ.m.t. um dulritun mikilvægra skjala sem send eru í tölvupósti og öryggisstig upplýsinga. (3.6)
    Ábyrgð: Forsætisráðuneyti, fjármálaráðuneyti, iðnaðar- og viðskiptaráðuneyti.

12. Auðkennd verði þau net- og upplýsingakerfi er varða þjóðaröryggi. Þau tekin út á grundvelli áhættu og veikleikagreiningar og öryggi þeirra samhæft. Ábyrgðaraðilar hvers kerfis tryggi öryggi þess. Komið verði á samstarfi ábyrgðaraðila við almannavarnaryfirvöld. (3.9.)
    Ábyrgð: Dóms- og kirkjumálaráðuneyti, Ríkislögreglustjóri, Póst- og fjarskiptastofnun.

13. Komið verði á fót nefnd til að huga að öryggi kerfa er varða þjóðaröryggi. Nefndin hafi formleg tengsl við almannavarnir eða Almannavarnaráð. Nefndin hafi samstarf við CERT-hópinn. (3.9)
    Ábyrgð: Dóms- og kirkjumálaráðuneyti, Ríkislögreglustjóri, forsætisráðuneyti.

14. Tryggð verði fjármögnun nýs fjarskiptastrengs er tryggi varasamband við útlönd. (3.10)
    Ábyrgð: Samgönguráðuneyti, forsætisráðuneyti

15. Póst- og fjarskiptastofnun setji reglur um öryggi og viðbúnað í almennum fjarskiptanetum sem taki til fjarskiptafyrirtækja, internetþjónustu og hýsingaraðila. (3.11.1)
    Ábyrgð: Póst- og fjarskiptastofnun.

III. Samstarf opinberra aðila og markaðarins um öryggismál verði eflt.

16. Póst- og fjarskiptastofnun hafi frumkvæði að því að koma á og skipuleggja CERT samstarf. Stofnunin annist slíkt samstarf, leggi til nauðsynlega aðstöðu og sjái um samráð við aðrar stofnanir ríkisins. (3.8)
    Ábyrgð: Póst- og fjarskiptastofnun.

IV. Unnið verði að því að bæta stjórnun upplýsingaöryggis með áhættumati og lágmarka áhrif utanaðkomandi ógna eða atburða.

17. Lokið verði sem fyrst innleiðingu á upplýsingaöryggisstaðlinum hjá stjórnarráðinu. (3.2)
    Ábyrgð: Öll ráðuneyti.

18. Stofnanir ríkisins sem vinna með viðkvæmar upplýsingar innleiði staðalinn um upplýsingaöryggi. Við mótun öryggisstefnu verði tekið mið af umfangi starfseminnar og áhættunni sem í henni felst. (3.2)
    Ábyrgð: Ríkisstofnanir.

V. Lögð verði áhersla á að efla erlent samstarf til varnar sameiginlegum ógnum.

19. Stjórnvöld taki virkan þátt í erlendu samstarfi er varðar net- og upplýsingaöryggi og miðli upplýsingum til innlendra aðila. (3.7)
    Ábyrgð: Samgönguráðuneyti, Póst- og fjarskiptastofnun.

VI. Eftirfylgni

Ábyrgð margra tillagna starfshópsins liggur hjá fleiri en einum aðila innan stjórnsýslunnar. Jafnframt eru tillögurnar þess eðlis að mislangan tíma tekur að framkvæma þær. Í ljósi þessa er lagt til að samgönguráðuneytið taki saman yfirlit yfir framkvæmd verkefna tveimur árum eftir birtingu skýrslunnar.
Ábyrgð: Samgönguráðuneyti

Tillögur um lagabreytingar

20. Í fjarskiptalög verði sett ákvæði er mæli fyrir um skyldu fjarskiptafyrirtækja til að skjalfesta hvernig staðið er að net- og upplýsingaöryggi ásamt heimild eftirlitsaðila til að framkvæma öryggisúttektir. (3.11.1)
    Ábyrgð: Samgönguráðuneyti.

21. Í fjarskiptalög verði sett ákvæði er banni að komið sé fyrir hugbúnaði í endabúnaði notanda án samþykkis þeirra. (3.11.2)
    Ábyrgð: Samgönguráðuneyti.

22. Að bannskrárákvæðið í 28. gr. persónuverndarlaga verði flutt í lög um Þjóðskrá eða því skipt upp og komið fyrir í fjarskiptalögum og póstlögum. Gerðar verði breytingar á 28 gr. persónuverndarlaga til samræmis þessu.
    Ábyrgð: Dóms- og kirkjumálaráðuneyti, samgönguráðuneyti.

23. Breytt verði 45. gr. fjarskiptalaga á þá leið að fjarskiptafyrirtækjum verði gert skylt að samkeyra símaskrár sínar við bannskrá Þjóðskrár.
    Ábyrgð: Samgönguráðuneyti.

24. Breytt verði orðalagi 5. mgr. 46. gr. laganna á þann veg að notendur almennrar tal- og farsímaþjónustu sem lið í markaðssetningu skuli virða bannskrá Þjóðskrár og bannmerkingar í símaskrám. Einnig verði kveðið á um rétt viðtakanda til að fá vitneskju um hvaðan þær upplýsingar koma sem liggja úthringingu til grundvallar.
    Ábyrgð: Samgönguráðuneyti

25. Bætt verði við nýjum efnisákvæðum í 33. gr. póstlaga á þá leið að:
    a. Markaðsaðilum sem hyggjast dreifa markpósti verði gert skylt að virða bannskrá Þjóðskrár.
    b. Skylt verði að nafn sendanda komi fram á áberandi stað á útsendum markpósti og hvert þeir sem andmæla því að fá slíkan markpóst geti snúið sér. Viðtakandi markpósts eigi rétt á að fá vitneskju um hvaðan þær upplýsingar koma sem liggja útsendingu til grundvallar.
    c. Dreifingaraðilum pósts ber að virða merkingar á póstkassa og bréfalúgu þar sem viðtöku markpósts og annars auglýsingaefnis er hafnað.
    Ábyrgð: Samgögnguráðuneyti.

26. Að kveðið verði á um, með skýrum hætti, að 1. mgr. 46 gr. fjarskiptalaga taki einnig til smáskilaboða (SMS). Jafnframt verði 5. mgr. laganna breytt í þá veru að hún taki ótvírætt til notkunar á farsíma við beina markaðssetningu þegar markpóstur er sendur með smáskilaboðum. (4.4)

    Ábyrgð: Samgönguráðuneyti.

27. Fellt verði brott ákvæði 14. gr. laga um húsgöngu og fjarsölu eða því breytt á þá leið að þar sé aðeins að finna almenna tilvísum til ákvæða fjarskipta- og póstlaga varðandi beina markaðssetningu.

    Ábyrgð: Iðnaðar- og viðskiptaráðuneyti.

28. Lagaskilyrði til útvarpsreksturs verði óháð tækni og samræmd almennum skilyrðum tíðniúthlutunar samkvæmt fjarskiptalögum. Um leið verði verkefni útvarpsréttarnefndar sameinuð starfsemi Póst- og fjarskiptastofnunar.

    Ábyrgð: Menntamálaráðuneyti, samgönguráðuneyti.

Nokkur algeng hugtök

DNS lénsheitakerfi, gagnasafn sem tengir saman IP-númer og lénsheiti.

CERT® Skrásett nafn Carnegie Mellon University, Pittsburg, alþjóðleg samtök sem bregðast sameiginlega við óvæntum atburðum sem varða öryggi á netkerfum.

CSIRT-hópur (Computer Security Incident Response Teams). Viðbragðshópur vegna óvæntra atburða er varða öryggi netkerfa. Venjulega skilgreinir hver hópur sín eigin markmið.

Fjarskipti er hvers konar sending og móttaka tákna, merkja, skriftar, mynda og hljóða eða hvers konar boðmiðlun eftir leiðslum, með þráðlausri útbreiðslu eða öðrum rafsegulkerfum.

Fjarskiptanet er sendikerfi og þar sem það á við skiptistöðvar, beinar og önnur úrræði sem gera mögulegt að miðla merkjum eftir þræði, þráðlaust, með ljósbylgjum, rafdreifikerfi, háspennulínum eða með öðrum rafsegulaðferðum, þ.m.t. net fyrir hljóð- og sjónvarp og kapalsjónvarp.

Endabúnaður (e. t*erminal equipment*) er sá búnaður (tölva) notanda sem er ekki hluti af fjarskiptakerfum en hluti af netkerfum.

Réttleiki (heilleiki, heilindi) (e. *integrity)* er staðfesting á að upplýsingum, sem eru sendar, mótteknar og vistaðar, sé á engan hátt breytt eða þær skertar. Þetta er aðferð sem tryggir að engu smáatriði sé hægt að hnika til frá því að gögnin voru upphaflega send.

Höfnun *(e. repudiation)* er aðferð sem tryggir að sendandi skjals geti ekki neitað því að hafa sent tiltekin skilaboð né móttakandi að hafa tekið á móti þeim. Þetta er afar mikilvægt þegar um rafræn viðskipti er að ræða.

Leyfisveiting (heimild)*(e. authorisation)* felur í sér leyfi til að framkvæma ákveðnar aðgerðir á gögnum sem eru vernduð. Dæmi um slíka leyfisveitingu er sú þjónusta sem bankarnir veita með heimabönkum.

Leynd (trúnaður)(e. c*onfidentiality*) merkir vernd tölvugagna gegn óviðkomandi aðilum, bæði á meðan gögnin eru send milli staða og þar sem þau eru vistuð.

Markpóstur Fjöldasending sem samanstendur einungis af auglýsingum, markaðskynningu eða almennu kynningarefni, hver sending eins að undanteknu nafni, heimilisfangi og kennitölu móttakanda sem og öðrum breytilegum upplýsingum sem ekki breyta innihaldi skilaboðanna sem send eru umtalsverðum fjölda móttakenda á þeim stað sem sendandi hefur áritað á póstsendinguna eða umbúðir hennar. Reikningar og reikningsyfirlit og aðrar sendingar sem hver fyrir sig er mismunandi skulu ekki teljast vera markpóstur.

Njósnahugbúnaður (e. spyware) hugbúnaður, sem laumað er inn, til að fylgjast með athæfi tölvunotenda.

Óumbeðin fjarskipti, notkun sjálfvirkra uppkallskerfa, símbréfa eða tölvupósts fyrir beina markaðssetningu þegar áskrifandi hefur ekki veitt samþykki sitt fyrir sendingunni fyrir fram.

RIX (Reykjavik Internet Exchange) er skiptistöð sem rekin er af Internet á Íslandi hf. (ISNIC) og þangað tengjast allir helstu internetþjónustuaðilar landsins.

Spilliforrit (e. malware, malicious software) er forrit sem er komið fyrir í vélbúnaði, fastbúnaði eða hugbúnaði og hefur þann tilgang að framkvæma einhverja heimildarlausa eða skaðlega aðgerð.

Smygildi (e. cookies) gagnahlutur sem vefþjónn vistar í geymslu notenda og hefur síðan aðgang að til að auðvelda samskipti. Oftast er smygildi vistað án vitundar notandans.

Staðfesting (upprunavottun)(e. *authentication)* er staðfesting á kennimarki til kerfis eða persónu. Slík staðfesting er meðal lykilatriða í UT-öryggismálum. Sá, sem biður um aðgang að gögnum, verður að geta sannað hver hann er t.d. með aðgangsorði, smart-korti eða búnaði sem þekkir líkamleg einkenni, svo sem augu eða fingraför.

Tiltækileiki *(e. availability)* merkir að gögn séu aðgengileg og þjónusta sé virk þrátt fyrir utanaðkomandi truflanir, svo sem rafmagnsleysi, náttúruhamfarir, slys eða árásir.

Trójuhestur (e. *Trojan horse*)er forrit sem virðist skaðlaust en hefur í sér spilliforrit sem leyfir heimildarlausa söfnun, fölsun eða eyðileggingu gagna.

Vefhlerunarbúnaður (e. web bugs) búnaður sem notaður er til að komast án heimildar yfir sendingu sem flytur upplýsingar.

Vefveiðar (e. phising) að fiska eftir persónuupplýsingum, svo sem aðgangsorðum og greiðslukortsnúmerum, með því að blekkja notendur.

Vistfang (e. address) er gildi sem tilgreinir stað.

Veira (e. virus) er forrit sem dreifir sér með því að breyta öðru forriti þannig að það geymir hugsanlega breytt afrit af fyrra forritinu og er innt þegar kallað er á smitaða forritið.

1. Inngangur

Fjarskiptanet og upplýsingakerfi eru orðin nauðsynlegur þáttur í daglegum störfum okkar og um leið grundvöllur að árangri í efnahagslífinu. Samruni fjarskipta- og upplýsingatækni gerir þessa þætti óaðskiljanlega og um leið viðkvæmari fyrir utanaðkomandi hættum. Þær geta verið af ýmsu tagi, t.d. inngrip í fjarskiptasendingar, ólögmætur aðgangur, truflanir á starfsemi netkerfa, dreifing skaðlegs hugbúnaðar sem breytir eða skemmir gögn, fölsun uppruna sendinga o.fl. Hætturnar takmarkast ekki við einstök ríki eða landamæri heldur geta þær átt uppruna hvar sem er í heiminum. Þá þarf að taka tillit til hættu af völdum náttúrunnar, gáleysistilvikum og ófullnægjandi hönnunar og frágangs fjarskiptamannvirkja.

Ófullnægjandi öryggi getur ekki einungis skaðað þann árangur, sem náðst hefur við uppbyggingu upplýsingasamfélagsins, heldur einnig efnahag og frelsi einstaklingsins í samfélaginu. Þetta kallar á sérstaka stefnumótun af hálfu stjórnvalda. Gera þarf úttekt á veikleikum net- og upplýsingakerfa og skipuleggja viðbrögðum við þeim. Einnig þarf að skilgreina ábyrgð opinberra aðila og aðila á almennum markaði m.a. gagnvart neytendum varðandi einstaka þætti á þessu sviði með það fyrir augum að tryggja ásættanlegt stig öryggis sem hæfir íslenskum aðstæðum.

Öryggi sendinga og réttleiki gagna er orðinn óhjákvæmilegur þáttur í rafrænni þjónustu, hvort sem hún er veitt af opinberum aðilum eða einkaaðilum, og vantrú á áreiðanleika og öryggi þjónustunnar hefur áhrif á útbreiðslu hennar. Því er nauðsynlegt að hver og einn gæti að öryggi sinna upplýsinga, gagna og kerfa með beitingu fullnægjandi tækni og aðferðum.

Einkaaðilar þurfa á grundvelli samkeppnis- og markaðssjónarmiða og frumkvæðis að bjóða úrval lausna sem samrýmast þörfum og kröfum markaðarins. Öryggi er og getur verið markaðs- og samkeppnistæki.

Hið flókna umhverfi net- og upplýsingaöryggis krefst þess að við stefnumótun á þessu sviði verði tekið tillit til pólitískra, efnahagslegra, skipulagslegra og tæknilegra þátta auk þess sem líta verður til eðlis starfseminnar sem er ekki miðlæg heldur alþjóðleg í eðli sínu.

Þess vegna verður að horfa til stefnumótunar ríkjanna í kringum okkur, sérstaklega til Evrópusambandsins sem heildar, þar sem þegar er til staðar víðtæk samræming og samstarf ríkja um þessi mál. Í þessu sambandi verður einnig að líta til þess að löggjöf innan EES hefur verið samræmd á sviðum net- og upplýsingaöryggis m.a. hvað varðar rammareglur um fjarskipti[1] (samskipti), um rafræn viðskipti[2] og um rafræna vottun[3].

Í gildandi löggjöf[4] eru lagðar kvaðir á aðila, sem veita fjarskiptaþjónustu, um að þeir taki tillit til tæknilegra og skipulagslegra þátta til að tryggja að öryggi sé í hæfilegu hlutfalli við áhættu.

Eins og komið er nánar að hér á eftir snýst net- og upplýsingaöryggi um að:
- tryggja aðgengi að þjónustu og gögnum,
- hindra truflanir og óheimil inngrip í sendingar,
- tryggja réttleika gagna sem hafa verið send, móttekin eða vistuð,
- tryggja leynd gagna,
- verja upplýsingakerfi gegn óheimilum aðgangi,
- vernd gegn árásum viðsjárverðs hugbúnaðar og manna,
- tryggja áreiðanleika staðfestinga.

[1] Lög um fjarskipti nr. 81/2003.
[2] Lög um rafræn viðskipti og aðra rafræna þjónustu nr. 30/2002.
[3] Lög um rafrænar undirskriftir nr. 28/2001.
[4] Sjá 2 og 3. mgr. 6. gr. og 1. mgr. 47. gr. laga um fjarskipti nr. 81/2003.

Til þess að taka á framangreindum þáttum eru lagðar til tillögur um aðgerðir sem miða að því að auka og viðhalda trausti á grunnstoðum upplýsingasamfélagsins á sviði net- og upplýsingaöryggis.

2. Um net og upplýsingaöryggi

Net- og upplýsingaöryggi er ekki aðeins spurning um tæknilega framkvæmd, þó að tæknilegar lausnir séu stór þáttur, heldur fyrst og fremst spurning um stjórnun og samræmda aðferðarfræði og síðan auðvitað fjárhagslegt bolmagn til framkvæmda. Alltof oft er litið á öryggismál sem óarðbæran hluta starfseminnar og forgangsraðað samkvæmt því.

2.1. Hvað er net- og upplýsingaöryggi?

Net- og upplýsingakerfi *(e. networks)* eru kerfi sem geyma upplýsingar, vinna þær og flytja gögn á tölvutæku formi. Þau innihalda bæði búnað sem sendir gögnin, svo sem kapla, radíóbúnað, gervihnetti, tölvubeina, gáttir, símstöðvar, og þá stuðningsþjónustu sem veitt er, t.d. lénakerfi og þjónustu sem ber kennsl á og staðfestir hver notandinn er. Netkerfunum tengist bæði búnaður sem verður stöðugt margþættari, t.d. tölvupóstur og netvafrarar, og sá endabúnaður sem tengdur er við þau, þ.e. símtæki og hvers konar tölvutengdur búnaður.

Net- og upplýsingaöryggi er hægt að skilgreina sem hæfni net- og upplýsingakerfa til að tryggja að ákveðin skynsamleg öryggismörk standist mannleg mistök og/eða tryggja að skemmdarstarfsemi hafi ekki áhrif á tiltækileika, staðfestingu, réttleika, rekjanleika og leynd gagna sem vistuð eru og send, eða þeirrar þjónustu sem veitt er um viðkomandi net- og upplýsingakerfi.

Allt sem getur haft áhrif á að net- og upplýsingakerfin, gögnin eða búnaðurinn virki eins og til er ætlast fellur undir þætti sem varða öryggi í upplýsingatækni.

2.2. Helstu ógnir

Hættur gegn net- og upplýsingaöryggi geta verið margs konar og þær geta átt uppruna hvar sem er í heiminum og hvenær sem er.

Hægt er að lama starfsemi fyrirtækja og einstaklinga með ýmsum aðferðum. Dæmi eru um aðferðir sem orsaka það að mikið af boðum frá tölvum, sem ekki eru rétt upp settar, eru send án vitundar eiganda þeirra á ákveðið netkerfi þannig að tölvubúnaður fyrirtækis hættir að geta veitt þjónustu. Misnota má persónu- og fjárhagsupplýsingar séu netkerfin ekki nægjanlega vernduð gegn innbrotum. Grípa má inn í sendingar netkerfa og afrita eða breyta gögnum. Algengasta og þekktasta ógnin hér á landi eru tölvuveirur.

2.2.1. Inngrip í fjarskiptasendingar

Hægt er að komast yfir rafrænar sendingar og breyta þeim eða afrita. Slík inngrip geta orðið með margvíslegum hætti, m.a. með aðgangi að vélbúnaði netkerfa eða með hlustun þráðlausra sendinga. Þeir hlutar kerfanna, sem viðkvæmastir eru fyrir slíkum inngripum, eru stjórnunarhlutar og tengipunktar eins og t.d. símstöðvar og netþjónar.

Þá er endabúnaður notenda í sífellt ríkari mæli sítengdur sem gerir möguleika til aðgangs að óvörðum tölvum auðveldari og dregur úr líkum á að árása verði vart.[5] Stórfelld aukning á þráðlausum netum, t.d. farsímanet, þráðlausum heimatengingum og þráðlausum innri netum, auðveldar óprúttnum aðgang.

Ólögmæt inngrip í fjarskiptasendingar eru aðför að friðhelgi einkalífs og geta falist í ólögmætri hagnýtingu gagna t.d. aðgagnsorðum, greiðslukortaupplýsingum vegna fjárhagslegs ábata eða til að valda skaða. Þetta er talin ein mesta hætta og hindrun fyrir víðtækri upptöku rafrænna

[5] Hér á landi eru um 80% virkra tenginga heimila sítengingar (ADSL, ljósleiðari, örbylgja eða um gervihnött).

viðskipta. Lausnir felast m.a. í aukinni vernd netkerfa, beitingu dulkóðunar og með breyttu vinnulagi.

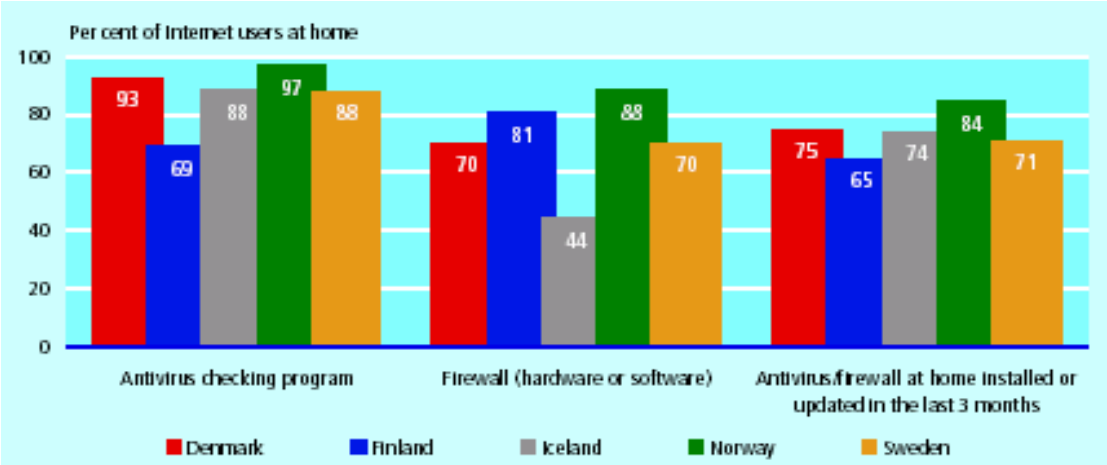
Fyrir fjarskiptafyrirtæki og þjónustuaðila er vernd netkerfa oft flókin og kostnaðarsöm framkvæmd. Verndin felst t.d. í bættri aðgangsstýringu að vél- og hugbúnaði og mannvirkjum ásamt leiðbeinandi reglum til starfsmanna.

2.2.2. Óheimill aðgangur

Undir þetta fellur ólögmætur aðgangur að tölvum og netkerfum, oftast í þeim tilgangi að hlera, afrita, breyta eða eyða gögnum. Þetta er gert með margvíslegum hætti, t.d. með inngripi í gögn sem fara um fjarskiptanetið og komast þannig yfir upplýsingar um aðgangsorð og aðrar persónulegar upplýsingar. Slíkt er stundum nefnt vefveiðar. Þetta má einnig gera með árásum á einstakar tölvur eða netkerfi.

Oft verða slík áreiti til þess að gera veikleika netkerfa sýnilega og opna augu þeirra aðila sem vilja fremja efnahagsbrot. Varnir gegn óheimilum aðgangi að persónuupplýsingum eins og fjárhags-, banka- heilbrigðis- og öðrum upplýsingum um einkamálefni einstaklinga er mikið hagsmunamál fyrir almenning og viðskiptalífið.

Tölvuvarnir heimila 2005.



Heimild: NSI statics, 2005 of ICY usage in housholds and by inviduals.

Tafla 1, sýnir öryggisvarnir heimila sem felast í veiruvörnum og eldveggjum (firewall). Eins og sést á töflunni eru eldveggir minnst notaðir á Íslandi miðað við hin Norðurlöndin.[6]

Helstu varnir á þessu sviði eru fólgnar í aðgangsstjórnun og eldveggjum en uppsetning þeirra verður sífellt einfaldari. Leita verður jafnvægis milli kostnaðar við varnir og hættunnar af árásum eða hugsanlegs tjóns af völdum þeirra.[7] Stöðugt þarf að fylgjast með að varnir séu í samræmi við breytingar á hættum og afleiðingum þeirra.

2.2.3. Truflun á virkni netkerfa

Algengt er að bilanir í netkerfum stafi af árásum aðila sem eru að kanna þolmörk eða veikleika kerfa eða hluta þeirra.[8] Árásir af þessu tagi hafa lítið beinst að talsímakerfum en því frekar að Internetinu eða einstökum hlutum þess. Í náinni framtíð má vænta þess að þetta breytist vegna frekari þróunar í IP-símtækni í gegnum tölvur.[9] Internetið styðst við svonefnt nafnaþjónskerfi

[6] Sjá, Nordic Information Society Statistics 2005, TemaNord 2005:562.
[7] Nefna má sem dæmi kröfur skattayfirvalda vegna framtala á netinu og bankastofnana hér á landi vegna aðgangs að heimabanka í gegnum netið.
[8] Veiruhöfundar eru þegar byrjaðir að búa sig undir að Microsoft setji á markað nýja stýrikerfiinu, Windows Vista, sem kemur á markað undir lok næsta árs. Austurrískur forritari bjó á dögunum til veiru, sem nota má til að herja á öryggisgalla í hugbúnaði, sem búist er við að verði notaður í nýja stýrikerfið.
[9] IP-síminn byggir á Internet Protocol samskiptastaðli sem fluttur er um almenna hluta Internetsins.

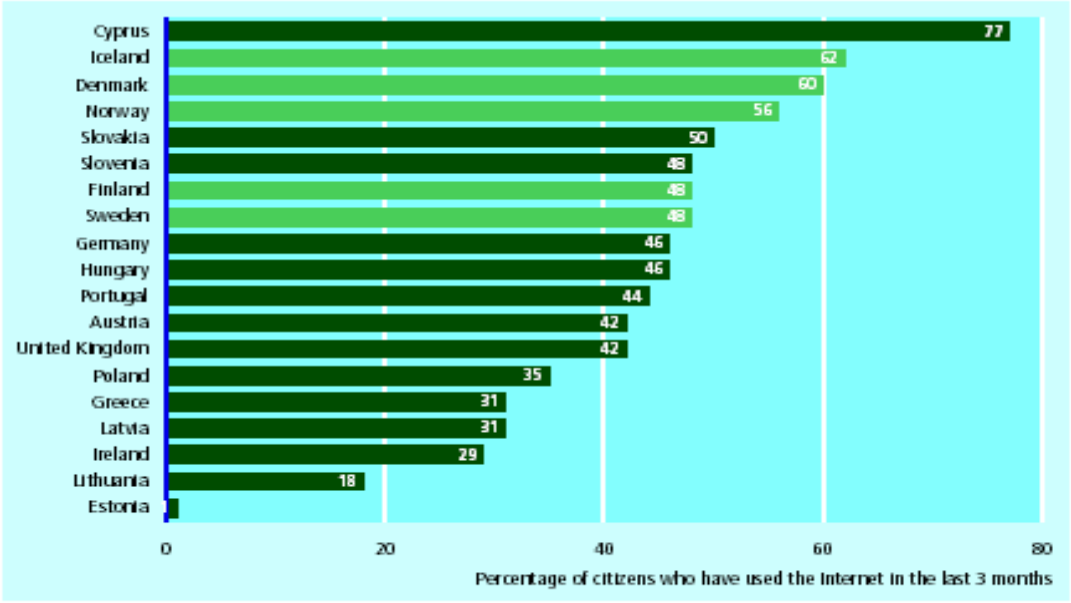
(e. Domain Name System, DNS). Árásir eða truflanir geta beinst að einstökum lénum, rótarlénum eða leiðarbeinum þó að oftast beinist þær að vefþjónum. Þær geta einnig falist í því að sent sé mikið magn gagna á einstaka tölvur þannig að þær hætti að geta veitt þjónustu (e. Denial of Service Attack, DoSA). Fjallað verður nánar um þetta síðar.

Árásir eða truflanir eins og hér var lýst geta valdið verulegu tjóni bæði fyrir netþjónustur og þá aðila sem stunda viðskipti um Internetið. Að öllu jöfnu á ekki að vera erfitt eða flókið að verjast árásum af þessu tagi með réttri uppsetningu á nafnaþjónskerfinu.

2.2.4. Skaðlegur hugbúnaður

Tölvuveirur eru ein alvarlegasta birtingarmynd skaðlegs hugbúnaðar. Slíkar veirur eru til í ótal gerðum og útgáfum sem ýmist valda tjóni á vél og hugbúnaði og sífellt koma fram nýjar útgáfur. Sumar veirur liggja í dvala fram að fyrirfram ákveðinni tímasetningu, svonefndar röksprengjur (e. logic bomb) eða verða virkar við ræsingu, svonefndir Trójuhestar. Enn aðrar veirur fjölfalda sjálfa sig og eru þær oft nefndar ormar. Samkvæmt alþjóðlegum samanburði eru heimili á Íslandi í fremstu röð í uppfærslu og notkun veiruvarnarbúnaðar.

Uppfærsla vírusvarna hjá almenningi á þrjá síðustu mánuði ársins 2004



Source: Eurostat, October 2005 (http://europa.eu.int/comm/eurostat/).
NSI statistics, 2005 surveys of ICT usage in households and by individuals.

Tafla 2, sýnir að Norðurlandabúar eru mjög duglegir við að uppfæra vírusvarnir sínar miðað við aðrar þjóðir Evrópu. Á þetta einkum við Ísland, Danmörk og Noreg.[10]

Skaði af völdum veira getur kostað ómælda fjármuni, m.a. í töpuðum vinnustundum. Helsta lausnin er öflugur varnarhugbúnaður sem leitar uppi og eyðir þekktum veirum og vel upplýstir notendur. Stöðugt verður að uppfæra hugbúnaðinn til að bregðast við nýjum veirum.

2.2.5. Fölsun á uppruna sendinga

Þegar notandi tekur á móti gögnum á Internetinu ber sendingin með sér hver sendandinn er. Jafnframt er gengið út frá því að þegar hringt er í gegnum Internetið eða póstur sendur á netfang um það berist hann á tilætlaðan áfangastað. Hægt er að falsa uppruna og einkenni tölvupóstsendinga (e. spoofing) þannig að leikmaður geri sér ekki grein fyrir því hver hinn raunverulegi sendandi er. Í mörgum tilvikum krefjast viðskipta- og eða persónuverndarhagsmunir þess að ríkari kröfur séu gerðar til staðfestingar á uppruna og leynd gagna.

[10] Sjá, Nordic Information Society Statistics 2005, TemaNord 2005:562.

Fölsun á uppruna getur valdið skaða með ýmsum hætti, t.d. með því að blekkja notendur til að sækja hugbúnað sem er skaðlegur eða afhenda trúnaðarupplýsingar til aðila sem villir á sér heimildir.[11] Vörn gegn slíku getur falist í upptöku rafrænna skilríkja og/eða aðferða sem tengjast dulritun gagnasambanda við heimasíður (e. Secure Socket Layer, SSL) en með því eru samskipti milli netþjónustunnar og notenda dulrituð.[12]

2.2.6. Náttúruhamfarir og gáleysisatvik

Margar þeirra ógna sem steðja að netkerfum stafa af náttúrulegum orsökum, t.d. veðri, flóðum, eldi, jarðskjálftum og eldgosum. Þær geta einnig stafað af gáleysisatvikum, t.d. vegna starfa á vegum verktaka[13] eða viðgerðaraðila (hugsanlega ófullnægjandi merkingar). Þá geta mannleg mistök rekstraraðila netkerfa leitt til rofs eða slita á sambandi.

Áföll vegna náttúruhamfara verða yfirleitt ekki séð fyrir, en þá myndast oftast hámarksálag á fjarskiptakerfin sem geta dottið út að hluta eða öllu leyti. Gera verður ráð fyrir áföllum af þessu tagi en við þau verður ekki að fullu ráðið. Rekstraraðilar net- og upplýsingakerfa verða að gera ráð fyrir áföllum sem þessum og koma á auka- eða varaleiðum[14] eða vera með viðbragðsáætlanir vegna möguleika á slíkum atvikum. Af þessu getur hlotist mikill kostnaður og leita þarf jafnvægis milli áhættu og kostnaðar m.a. með áhættugreiningu og samstarfi eða samvinnu milli fyrirtækja um þá þætti.[15] Draga má úr hættu á mannlegum mistökum með aukinni þjálfun starfsmanna og með því að fyrirtæki komi sér upp sérstakri öryggisstefnu sem þau fylgi.

3. Stefnumótun

Upplýsinga- og fjarskiptatækni og tækifærin sem hún skapar eru einn helsti drifkrafturinn og meginstoðin að baki upplýsingasamfélaginu, þar sem söfnun og miðlun upplýsinga skiptir sífellt meira máli fyrir samfélagið bæði í efnahagslegu og félagslegu tilliti. Í þeim tækifærum sem tæknin færir okkur leynast einnig hættur sem kalla á aukna vernd upplýsinga og gera öryggi netkerfa mikilvægara. Þetta eru hættur sem varða öryggishagsmuni allra í samfélaginu og sem stjórnvöld, fyrirtæki og einstaklingar verða að verjast. Mikilvægt er að tryggja að þessi stoð samfélagsins virki sem best og það kallar á sérstaka aðkomu og stefnumótun af hálfu stjórnvalda.

Með stefnumótun á sviði net- og upplýsingatækni, aukinni notkun staðla sem stuðla að samhæfðum vinnubrögðum, gerð leiðbeiningarefnis, árvekni og samvinnu allra þátttakenda og skýrum skilum milli ábyrgðar einstakra þátttakenda á sviðinu er leitast við að bæta net- og upplýsingaöryggi. Horft hefur verið til þess sem aðrar þjóðir hafa verið að gera, sérstaklega Norðurlöndin og aðrar Evrópuþjóðir, auk viðmiða eða viðhorfa OECD[16] og ESB[17].

Leggja verður áherslu á nýja hugsun og hegðun þegar við eigum í rafrænum upplýsingaskiptum eða samskiptum í gegnum net- og upplýsingakerfi. Einn mikilvægasti þátturinn í að bæta öryggi á þessu sviði er að allir sem að málum koma séu meðvitaðir um

[11] Dæmi eru um markaðssetningu á hugbúnaði sem sérstaklega er ætlað að breyta eða dylja uppruna sendinga.
[12] Þessi tækni styðst við allt að 168 bita dulritun.
[13] Fjölmörg dæmi eru um þetta, t.d. rof á sambandi við ljósleiðara Farice í Skotlandi í lok júní 2005.
[14] Leggja verður aukna áherslu á aukaleiðir í stað varaleiða þannig að netkerfi verði hönnuð með fleiri en einni virkri leið milli tveggja staða á hverjum tíma. Varaleiðir, sem aðeins eru virkjaðar vegna bilana, henta ekki í pakkaskiptum netum eins og Internetinu.
[15] Sjá t.d. 72. gr. laga um fjarskipti varðandi heimildir til að takmarka tiltekin fjarskipti og einnig til að nota fjarskiptavirki í þágu björgunaraðila.
[16] OECD Guidelines for the Security of Information Systems and Networks, Towards a Culture of Security, OECD 2003.
[17] Sjá, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Network and Information Security: Proposal for A European Policy Approach, COM(2001) 298 final, Brussels, 6.06.2001.

hætturnar, varnir gegn þeim og geri sér líka grein fyrir hvaða hættum þeir sjálfir hafa stjórn á. Jafnframt þessu þarf að gera aðgengilegar upplýsingar um aukið öryggi, reka áróður fyrir öryggisstefnu, viðurkenndum starfsháttum og viðbrögðum við öryggisbrestum. Auka þarf hæfni allra þjóðfélagsþegna til að takast á við verkefnið.

Vinna verður að því með markvissum hætti að þróa öryggisvitund í samfélaginu.

Allir þátttakendur í upplýsingasamfélaginu verða að geta treyst á áreiðanleika og réttleika þess svo að það megi þróast áfram ótruflað til hagsbóta fyrir allt samfélagið.

Leggja verður áherslu á að byggja upp traust á upplýsingasamfélaginu, öryggi innviða þess og samkeppnishæfni.

Nauðsynlegt er að auka samvinnu, miðlun upplýsinga og samstarf milli opinberra aðila og aðila á markaðinum um öryggismál, m.a. með því að samræma stefnu, ábyrgð, markmið og þannig ná betri árangri og hagnýtingu fjármuna við framkvæmd öryggismála. Þá má lágmarka áhrif utanaðkomandi ógna eða atburða með markvissu samstarfi og samvinnu í viðbrögðum m.a. í gegnum CERT-hópa.

Efla þarf samstarf opinberra aðila og markaðarins um öryggismál.

Með áhættumati, þar sem ógnir og veikleikar eru metnir með tilliti til tækni, umhverfis og mannlegra þátta, þjónustu þriðju aðila, stefnu o.s.frv., má bæta öryggi með markvissri og hagkvæmri nálgun. Hægt er að greina áhættu og viðunandi stig viðbragða til að draga úr henni í ljósi mikilvægis upplýsinganna sem verið er að vernda og hugsanlegs tjóns.

Nauðsynlegt er að bæta stjórnun upplýsingaöryggis með áhættumati og áhrif utanaðkomandi ógna eða atburða verði lágmörkuð.

Rafræn samskipti eiga sér engin landamæri ekki frekar en Internetið. Barátta fyrir auknu öryggi í því umhverfi er því áskorun fyrir allar þjóðir. Líta verður á net- og upplýsingaöryggi sem viðfangsefni sem ekki verður eingöngu tekist á við með aðgerðum hérlendis heldur verður lausnin að byggjast á alþjóðlegu samstarfi. Slík samvinna fellst m.a. í innleiðingu og notkun staðla, stefnumótun og samvinnu um öryggismál og beinni þátttöku í alþjóðasamstarfi, þ.m.t. í Net og upplýsingastofnun Evrópu (European Network and Information Security Agency, ENISA).[18]

Leggja verður áherslu á að efla enn frekar erlent samstarf til varnar sameiginlegum ógnum.

3.1. Verndun innviða netkerfa

Það samfélag sem við búum við í dag þrífst ekki nema samgöngu- og veitukerfi og almannaþjónusta samfélagsins séu virk. Stór hluti þeirra, orka, vatn, flug-, skipa- og landflutningar, heilsuvernd, löggæsla, banka- og verðbréfaþjónusta, neyðarþjónusta (112) auk stjórnarráðsins, byggja á og styðjast við samskipta- eða fjarskiptanet. Eldri og oft handvirkar aðferðir eru í sífellt ríkara mæli leystar af hólmi með ódýrari, opnari, skilvirkari og langtum útbreiddari tengingum gegnum Internetið. Hættur sem áður fólust í árásum eða skemmdum á efnislegum þáttum, eiga sér nú stað rafrænt og oftast með miklu áhrifaríkari hætti.

Gera þarf úttekt á og auðkenna þau netkerfi sem skipta máli fyrir samfélagið sem heild, m.a. á grundvelli áhættu- og veikleikagreiningar. Ábyrgðaraðilar á hverju sviði verða að axla ábyrgð

[18] Ríkisstjórn Íslands tók ákvörðun um þátttöku Íslands í ENISA-stofnuninni fyrrihluta ársins 2004.

á öryggi eigin kerfa og koma verður á samstarfi þeirra við almannavarnaryfirvöld. Sjá nánar um þetta í kafla 3.9.

Sérstaka áherslu verður að leggja á vernd talsíma og gagnaflutningsneta, m.a. með tilliti til þess að tal mun halda áfram að færast yfir á IP-net (VoIP). Vernda verður innviði netkerfa sem skipta miklu máli fyrir samfélagið, til að tryggja tiltækileika, réttleika og leynd. Aðgerðir til að tryggja öryggi verða að gera ráð fyrir að kerfin virki eins og til er ætlast. Fjarskiptafyrirtæki verða að sjá um að gera eigin áætlanir og skipuleggja viðbrögð við atburðum sem eiga sér stað eða geta átt sér stað í þeirra eigin netkerfum.

Til að auka öryggi þarf að tryggja að farið sé að reglugerðum og stöðlum á sviði bygginga-, tölvu- og fjarskiptatækni vegna frágangs á lögnum í hús, heimtaugum, húskössum[19], götulögnum, lögnum jarðstrengja sem og öðrum þáttum er lúta að ytra öryggi svo sem frágangi og aðgengileika bygginga.

3.1.1. Áhættumat

Upplýsingar eru í eðli sínu verðmæti sem mikilvægt er að vernda líkt og aðrar mikilvægar eignir í rekstri. Mikilvægt er að beitt sé viðurkenndum aðferðum eða aðferðarfræði til að auðvelda vernd þessara eigna og um leið auðvelda hagkvæma og raunhæfa útfærslu á upplýsingaöryggi. Þetta á sérstaklega við um fyrirtæki [20] sem eiga verðmæti í upplýsingum og þurfa að útfæra eða aðlaga starfsemina til að verja þær. Ólíkt því sem margir halda snýst upplýsingaöryggi ekki nema að litlum hluta um tækni þó að hún sé nauðsynlegur þáttur þess. Upplýsingaöryggi snýst að verulegu leyti um menningu, stjórnun og aðferðarfræði, en jafnframt verður að hafa í huga að upplýsingaöryggi er síbreytilegt.

Áður en áhættumat getur farið fram er nauðsynlegt að flokka net- og upplýsingakerfi með tilliti til þess hversu mikilvægt kerfið/upplýsingarnar eru og hvaða ógnir gætu steðjað að þeim. Tilgangurinn væri að einfalda vinnu og með því að tengja þær öryggisráðstafanir, sem gripið er til við viðkomandi flokk, það gæti minnkað kostnað vegna net- og upplýsingaöryggis. Fjölda flokka mætti ákveða af ábyrgðaraðilanum sjálfum, sem og til hvaða upplýsinga eða kerfa þeir skulu ná til. Eignaskrá kemur fram í öryggisstefnu viðkomandi aðila.

Samkvæmt BS 7799-2:2002[21] öryggisstaðlinum er áhættumat heildarferli áhættugreiningar og áhættuvægismats. Metnar eru ógnir sem steðja að upplýsingum og upplýsingavinnslu, áhrif ógna á eignir eru metnar sem og viðkvæmni eigna gagnvart ógnum. Einnig eru metnar líkur á að ógnir leiði til áfalla í rekstri. Metin er hættan á því að óviðkomandi fái aðgang að upplýsingum, geti breytt upplýsingum eða skert öryggi þeirra að öðru leyti. Áhættumat tekur einnig til athugunar á umfangi og afleiðingum hættunnar m.t.t. eðlis þeirra upplýsinga sem unnið er með. Áhættumat getur bæði verið einfalt eða flókið, allt eftir eðli starfseminnar sem í hlut á. Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum og mikilvægt er að endurskoða áhættumat reglulega til að tryggja yfirsýn stjórnenda og raunhæft val á öryggisráðstöfunum.

Lega landsins á Norður-Atlantshafssprungusvæðinu, þar sem u.þ.b. 25% þess er á skilgreindu eldvirku svæði þ.m.t. hafsvæðinu í kringum landið, verður að teljast stór áhættuþáttur út frá öryggissjónarmiðum. Þetta kallar á sérstakar kröfur við lagningu jarðstrengja, staðsetningu radíóbúnaðar og símstöðva og varaleiða er taka mið af þessari hættu. Flóð, samfara eldvirkni,

[19] Fjarskiptalagnir í húsnæði áskrifenda, þ.m.t. húskassar, eru á ábyrgð húseigenda. Póst- og fjarskiptastofnun er ætlað að setja reglur um frágang húskassa og lagna í þeim tilgangi að tryggja vernd fjarskipta og skilgreina aðgangsheimildir.

[20] Þegar talað er um fyrirtæki er að öllu jöfnu átt við fyrirtæki og stofnanir nema annað sé tekið fram.

[21] Í lok síðasta árs urðu breytingar á upplýsingaöryggisstöðlunum ISO 17799 (leiðbeiningastaðlinum) og BS 7799 (kröfustaðlinum): ISO 17799:2000 varð ISO 17799:2005 og BS 7799-2:2002 varð ISO 27001:2005. Þessir staðlar komu út júlí 2006.

eldgos og jarðskjálftar, hafa eyðilagt mannvirki og haft áhrif á fjarskiptakerfið og það er ástæða til að skoða alla verkferla í því samhengi.

Lagt er til að þessum málum verði gefinn sérstakur gaumur af nefndinni sem fjallað er um í kafla 3.9.

3.1.2. Mikilvægi nafnaþjónskerfa, lénamál

Við samskipti á Internetinu er stuðst við vistföng. Með þeim er borin kennsl á ákveðinn nettengipunkt fyrir samband sem er notað til að beina sendingum um Internetið. Vistfang er forsenda þess að sendingar rati rétta leið um Internetið

IP-vistfang er númer samkvæmt IP-samskiptastaðlinum (e. Internet Protocol) sem hverju tæki, sem tengist Internetinu, er úthlutað. IP-vistfang er 32 bita heiltala sem oft er rituð sem fjórar 8 bita heiltölur til þæginda fyrir notendur (IPv4 staðall og unnið er að innleiðingu nýs IPv6 staðals). Við samskipti á Internetinu styðjast notendur þó að jafnaði ekki við IP-vistfangið þegar þeir velja samband við annan notanda eða þjónustu heldur nafn sem samanstendur af bókstöfum, tölustöfum og táknum sem notuð eru til þess auðkenna endanlegan notanda (netfang).

Hið tvöfalda kerfi númera og nafna í Internetinu hefur í för með sér að notandi verður að tengjast nafnþjóni, sem flettir upp IP-vistfangi (númerinu) sem samsvarar nafninu sem notandinn hefur valið (netfanginu)..

Við öra fjölgun tölva reyndist erfitt að halda utan um IP-vistföngin og því var komið á nafnkerfi sem hægt var að varpa yfir í IP-númer. Þetta kerfi var endurskoðað á tíunda áratug síðustu aldar og voru þá samdar meginreglurnar fyrir lénafyrirkomulagið, DNS, sem birtust í Internet staðlinum RFC 920. Staðallinn gerði ráð fyrir annars vegar 7 almennum topplénum (generic top level domains), þ.e. .com, .net, .org, .mil, .gov, .edu og .int, og hins vegar landslénum sem eru tveggja stafa og taka mið af staðlinum ISO 3166.[22]

Til þess að rafræn viðskipti í gegnum Internetið gangi er nauðsynlegt að notendur beri traust til öryggisráðstafana í netinu. Verndun upplýsinga um lén og verndun persónuupplýsinga munu hugsanlega krefjast endurskoðunar eða setningu opinberra reglna um úthlutun og skráningu léna.

Skráning og úthlutun nafna undir landsléninu .is er í höndum Internets á Íslandi hf, ISNIC. Starfsemi fyrirtækisins er tvíþætt en það sér einnig um rekstur á skiptistöð íslenskra internetþjónustuaðila (RIX), þar sem þeir geta skipst á IP-umferð sín á milli og komið þannig í veg fyrir að innanlandsumferð flæði um útlandasambönd. Skiptistöðin er hlutlaus tengipunktur þar sem aðilar, sem uppfylla ákveðin skilyrði, tengjast og geta með gagnkvæmum samningum skipst á umferð við aðra RIX-aðila. Þessir tveir þættir starfseminnar tengjast þó lítið, eru hvor öðrum óháðir þannig að ef rekstur RIX stöðvast þá truflast DNS þjónustan ekki og öfugt (DNS gagnagrunnurinn er speglaður á öðrum stöðum).

Við RIX er tengt eintak af einum af 13 rótarnafnaþjónum heimsins en það er gert til að tryggja snuðrulusan rekstur nafnakerfisins innanlands ef netsamband við útlönd rofnar um lengri tíma. Starfsemi skiptistöðvarinnar er mikilvæg og allir, sem tengjast Internetinu, eiga mikið undir því að þessi starfsemi gangi ótrufluð.

Mikilvægt skref hefur þegar verið stigið í bættu öryggi með því að afrit af gagnagrunni fyrir nafnaþjónustu (DNS) hefur nú verið vistað á öðrum stað. Vegna mikilvægis þessarar starfsemi þarf að gæta sérstaklega að ytra öryggi hennar og að fyrir liggi áhættugreining vegna starfsemi nafnaþjónsins og virkni Internetsins í því sambandi.

[22] Nafnakerfi netsins er lýst í STD13 (RFC1034 0g RFC1035) með síðari viðbótum í RFC4033, RFC4034 og RFC4035. Hlutverki kerfisins ef lýst í RFC3467.

3.2. Staðlar og vottun

Mikilvægt er að vinna skipulega og með samræmdum hætti að net- og upplýsingaöryggi. Sérstakir staðlar hafa verið mótaðir til að ná þessum markmiðum. Sá staðall sem stuðst hefur verið við hér á landi er ÍST ISO/IEC 17799:2000[23] um stjórnun upplýsingaöryggis. Samkvæmt honum ber að móta öryggisstefnu, framkvæma áhættugreiningu og skjalfesta þær öryggisráðstafanir sem gripið er til á grundvelli greiningarinnar. Nauðsynlegt er að fyrirtæki og stofnanir sem vinna með mikilvægar upplýsingaeignir hagi net- og upplýsingaöryggi sínu í samræmi við kröfur staðalsins.

Í gildi eru reglur Persónuverndar nr. 299/2001 um öryggi persónuupplýsinga sem kveða á um lágmarkskröfur varðandi hýsingu og vinnslu persónuupplýsinga. Þessar reglur taka mið af staðlinum. Þær ná hins vegar ekki til net- og upplýsingaöryggis almennt. Til að tryggja það sem best er mikilvægt að settar séu samsvarandi reglur sem taki til starfsemi fjarskiptafyrirtækja.

Stjórnarráðið hefur þegar hafið innleiðingu á staðlinum og nauðsynlegt er að ljúka því verki sem fyrst. Enn fremur er mikilvægt að innleiða staðalinn hjá þeim stofnunum ríkisins sem vinna með viðkvæmar upplýsingar. Hugsanlegt er að smærri ríkisstofnanir geti átt samstarf um kaup á þjónustu sem auðveldar þeim að uppfylla kröfur um öryggi í samræmi við staðalinn. Jafnframt þarf að huga að netnotkun starfsmanna og umgengni þeirra um tölvupóst. Hafa má til hliðsjónar vinnureglur Persónuverndar um netnotkun starfsmanna sinna.[24]

3.3. Vitundarvakning

Notendur verða að skilja mikilvægi öryggis og gera sér grein fyrir öryggistengdum kröfum. Í reynd verður heildin ekki sterkari en veikasti hlekkurinn. Þeir notendur, sem ekki eru meðvitaðir um þetta, verða að veikum hlekk í keðju netöryggis. Þekkingaskortur eða gáleysi á þessu sviði er ekki bara líklegt til að valda tjóni hjá viðkomandi notanda heldur er það einnig líklegt til að valda öðrum skaða. Það er viðurkennd staðreynd á sviði öryggismála að notendur, sem eru vel upplýstir um hættur og hvernig megi verjast þeim, eru besta vörnin. Því verður að leggja áherslu á aukna fræðslu og miðlun upplýsinga til almennings um net- og upplýsingaöryggi.[25]

Það er á ábyrgð hvers og eins að verða sér úti um nægjanlega þekkingu til að tryggja öryggi netkerfa og gagna eða verða sér úti um þjónustu sem tryggir það. Það er hins vegar verkefni allra sem að þessum málum koma að auka þekkingu á þessu sviði. Mikilvægt er að fjarskiptafyrirtæki, þ.m.t. netþjónustuaðilar, eftirlitsaðilar, önnur stjórnvöld og félagasamtök, sem að þessum málum koma, samræmi upplýsingagjöf til almennings um þá þætti net- og upplýsingaöryggis er máli skiptir. Jafnframt að þessir aðilar vinni saman að gerð leiðbeiningarefnis til dreifingar til almennings og í skólum. Nauðsynlegt er að stjórnvöld séu virk í þessu starfi.[26] Eðlilegt er að Póst- og fjarskiptastofnun verði falið frumkvæðis- og samræmingarhlutverk á þessu sviði.

Fræðsla í þessum málum þarf einnig að felast í upplýsingum um hvert almenningur geti snúið sér með umkvartanir sínar t.d. vegna óværu, ónæðis eða hugsanlegra lögbrota í tengslum við þessi mál.

---

[23] http://www.stadlar.is/Apps/WebObjects/Stadlar.woa/2/wa/dp?numer=17799&NewLook.19.0.1.1=Leita&name=stadlaskra&wosid=yc70OEYt2856KJqVtnVxQM

[24] http://www.personuvernd.is/tolvunefnd.nsf/pages/233959C93874FEB400256CD80055B1A3

[25] Samtökin Heimili og skóli hafa unnið markvisst að fræðslu varðandi öryggi á netinu. Sú fræðsla hefur beinst að grunnskólabörnum og foreldrum þeirra, ásamt skólum, skólayfirvöldum, stjórnvöldum, netþjónustuaðilum og fjölmiðlum.

[26] Þess má geta að samkvæmt stefnu ríkisstjórnarinnar í málefnum upplýsingasamfélagsins á miðlun leiðbeininga og fræðsluefnis um öryggismál, neytendavernd, persónuvernd og siðferðileg álitaefni, að vera aðgengileg á netinu. Póst- og fjarskiptastofnum birtir upplýsingar um öryggismál á vefsíðunni www.netoryggi.is.

Fyrst og fremst hefur verið litið til net- og upplýsingaöryggis út frá virkni netkerfa og verndun upplýsinga en ekki með tilliti til efnisinnihalds og siðferðislegra spurninga er varða þau mál. Víða erlendis er í gangi svartlistun á heimasíðum er innihalda klám (barnaklám) og annað ósiðlegt og um leið ólöglegt efni. Í Noregi er t.d. öflugt starf í gangi á vegum lögregluyfirvalda í samstarfi við netþjónustuaðila við svartlistun á heimasíðum sem innihalda ólögmætt efni. Notandinn fær aðvörun á skjáinn ef hann ætlar inn á slíka síðu. Ekki er tekin sérstök afstaða til þessa álitaefnis enda heyrir málefnið undir réttarvörsluaðila hér á landi[27]. Sjálfsagt er að þeir neytendur sem það vilja geti fengið aðgang að slíkri þjónustu frá netþjónustuaðilum. Eðlilegt er þó að í almenningsbókasöfnum, grunn- og framhaldsskólum sé reynt að takmarka aðgang að ólögmætu og eða ósiðlegu efni í gegnum slíka þjónustu eða með öðrum takmörkunum.

3.3.1. Ábyrgð og upplýsingar til neytenda

Gera verður kröfu til þeirra fyrirtækja sem starfa á sviði fjarskipta- og upplýsingatækni, að þau upplýsi almenning um veikleika rafrænna samskipta, t.d. um þráðlaus net, og mikilvægi þess að notaður sé samskiptamáti sem tekur mið af mikilvægi sendinga.[28] Það er mikilvægt að fyrirtækin þjóni viðskiptavinum sínum annars vegar með fullnægjandi leiðbeiningum við upphaf viðskipta og síðan með ítarefni á heimasíðum sínum eða með kræjum inn á heimasíður með leiðbeiningum um veiruvarnir, eldveggi, ruslpóst og aðra hluti er varða veikleika netsamskipta almennings. Verulega hefur skort á í þessu þó að takmarkaðar og dreifðar upplýsingar sé á stöku stað. Gera verður sérstakt átak til að bæta úr þessu. Í fjarskiptalögum er að finna ákvæði sem heimila Póst- og fjarskiptastofnun að leggja kvaðir á fjarskiptafyrirtækin[29] í þessum efnum, sbr. ákvæði t.d. um skilmála og gjaldskrár (37. gr.), reikninga (38. gr.), gæði þjónustu (41. gr.) og í IX. kafla laganna um vernd persónuupplýsinga og friðhelgi einkalífs.

Til að efla net- og upplýsingaöryggi verða seljendur vél- og hugbúnaðar einnig að axla ábyrgð gagnvart viðskiptavinum sínum og samstarfsaðilum. Þeir sem selja vélbúnað og hugbúnað verða að fylgja viðurkenndum öryggisvenjum og stöðlum ásamt því að gera grein fyrir öryggiseiginleikum og kröfum sem gerðar eru um rétta notkun viðkomandi búnaðar.

Lagt er til að seljendum tækja og búnaðar og þjónustu sé skylt að upplýsa kaupanda eða notanda þjónustu um þá þætti sem skipta máli varðandi örugga notkun, um helstu veikleika og hvernig best sé að varast þá og geri efnið aðgengilegt, t.d. á heimasíðum sínum.

3.4. Menntun og fræðsla

Menntun í öryggismálum fjarskipta- og upplýsingakerfa er órjúfanlegur þáttur í hagnýtingu tölvutækni í skólastarfi, allt frá leikskóla til háskóla. Leggja ber sérstaka áherslu á vitund skólabarna á leikskóla- og grunnskólaaldri um þær sérstöku hættur sem kunna að vera samfara tölvunotkun þeirra og stuðla að betri þjálfun barna í öruggri tölvunotkun. Mikilvægt er að upplýsingum um örugga tölvunotkun sé miðlað til foreldra, en ástæða er til að ætla að í mörgum tilvikum skorti þá upplýsingar um þessi atriði.

Styðja ber við framangreindar áherslur með því að tiltaka öryggismál sérstaklega við hagnýtingu upplýsingatækni í skólastarfi og tiltaka fræðsluskyldu á því sviði í aðalnámskrám fyrir leikskóla og grunnskóla. Við gerð námsefnis verði haft samstarf á milli menntamálaráðuneytis, Póst- og fjarskiptastofnunar og félagasamtaka á borð við Heimili og

[27] Benda má á að heimildir er að finna í fjarskiptalögum til að bregðast við með þessum hætti Í 6. gr. laganna er kveðið á um skilyrði almennrar heimildar til fjarskiptastarfsemi og í h-lið 2. mgr. er síðan upptalning á skilyrðum m.a. um takmarkanir að því er varðar sendingu á ólöglegu innihaldi og takmarkanir á skaðlegu innihaldi sjónvarpsefnis.

[28] Benda má á skyldu fjarskiptafyrirtækja skv. 1. mgr. 47. gr. fjarskiptal. um að upplýsa notendur ef hætta er á að leynd fjarskipta verði rofin.

[29] Sjá t.d. f, g, h og o-liði 6. gr. fjarskiptalaga sbr. og reglur nr. 345/2005 um almenna heimild til að reka fjarskiptanet eða fjarskiptaþjónustu.

skóla um útgáfumál og kynningar í skólum og meðal almennings. Þannig mun nýtast sú þekking og reynsla sem þegar er fyrir hendi á þessu sviði.

Efling rannsókna á sviði öryggis í fjarskipta- og upplýsingakerfum er forsenda fyrir því að unnt sé að undirbúa námsframboð á því sviði. Lagt er til að stjórnvöld veiti fjármunum til rannsókna á þessu sviði t.d. með því að stofna tímabundna rannsóknarstöðu doktorsnema í samstarfi við þá háskóla sem bjóða upp á kennslu í tölvunarfræðum. Með slíkum rannsóknum verði undirbúinn frekari jarðvegur fyrir meistaranám á þessu sviði, jafnframt því sem þáttur öryggismála verði efldur í núverandi kerfisfræði- og tölvunarfræðinámi.

Samhliða framangreindum ráðstöfunum er æskilegt að stuðla að samstarfi hins opinbera, samtaka og markaðsaðila þannig að atvinnurekendur geti boðið upp á námskeið fyrir starfsfólk í öryggismálum. Markmið slíkra námskeiða væri að styrkja hæfni í net- og upplýsingaöryggi alls samfélagsins.

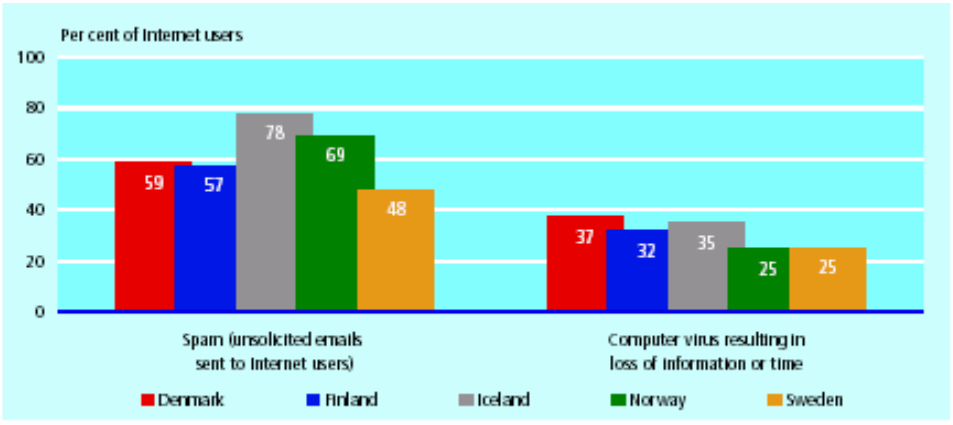
3.5. Ruslpóstur

Öll óumbeðin fjarskipti eru óheimil lögum samkvæmt. Gagnlegt er að gera greinarmun á ruslpósti (spam) annars vegar og markpósti hins vegar enda eðli þeirra er þó að mörgu leyti ólíkt.

Benda má t.d. á eftirfarandi atriði sem greinir ruslpóst frá markpósti:

- Að baki ruslpósts standa oftast ekki nein fyrri viðskipti eða samskipti ólíkt markpósti,
- sendandi ruslpósts villir oft á sér heimildir á meðan sendandi markpósts gerir það ekki,
- oftast er ekki hægt að rekja ruslpóst, þ.e. ekki kemur fram hver sé sendandi meðan markpóstur ber það yfirleitt með sér,
- við sendingu ruslpóstsins hefur póstföngum oftast verið aflað í söfnun með skipulegum hætti af netinu, án samþykkis *eiganda* póstfangsins,
- ekki er hægt að afþakka ruslpóst og ef það er gert þá verður það til þess að auka verðmæti netfangsins í sölu til frekari dreifingar,
- innihald ruslpósts oft ósiðlegt eða felur í sér framboð vöru með ólögmætum hætti eða af vafasömum uppruna, ólíkt markpósti,
- magn ruslpósts getur valdið hættu fyrir virkni netkerfa (magnpóstur),
- markpóstur er oft póstur sem óskað hefur verið sérstaklega eftir á meðan ruslpósturinn er eitthvað sem enginn vill fá.

Öryggisvandamál tengd internetnotkun s.l. 12 mánuði 2005



Source: NSI statistics, 2005 surveys of ICT usage in households and by individuals.

Tafla 4. Stór hluti notenda Internetsins á Norðurlöndum hafa fengið ruslpóst (spam) – flestir frá Íslandi og Noregi en fæstir í Svíþjóð (ekki spurt um tíðni eða viðbrögð notenda). Tölvuveirur sem leiða til missis upplýsinga eru mun sjaldgæfari en ruslpóstur en eru líklegri til að valda meiri vanda þegar það gerist.[30]

[30] Sjá, Nordic Information Society Statistics 2005, TemaNord 2005:562.

Segja má að stjórnvöld hafi hvorki tæki, tól né úrræði til að takast á við ruslpóstinn með virkum hætti, burtséð frá lagaúrræðum sem þegar eru flest til staðar. Þau hafa ekki skilað árangri að þessu leyti, enda vandamálið alþjóðlegt og ekki verður tekist á við það með aðgerðum er takmarkast við landamæri einstakra ríkja. Ekki er þó að finna ákvæði sem heimilar að pósti sé hent, frekar en að bréfbera eða þeim sem flokka almennan bréfpóst sé heimilt að fleygja honum. Skilmálar netþjónustuaðilans virðast fyrst og fremst miðast við að þjónustan sé ekki notuð til að senda slíkan póst og taka við svörum við honum.[31] Þrátt fyrir þetta liggur fyrir að stærstur hluti tölvupósts berst aldrei á áfangastað. Netþjónustuaðilar hér á landi fleygja u.þ.b. 85% af öllum pósti sem berst gegnum Internetið. Af þessu er stærstur hluti stöðvaður í gegnum samstarf netþjónustuaðila (svartlistun) og afgangurinn með skimun leitarorða hjá þjónustuaðilanum sjálfum. Þetta er fyrst og fremst þjónusta við notendur og er í flestum tilvikum hluti af staðlaðri uppsetningu (stillingu) við upphaf þjónustu. Óska þarf sérstaklega eftir lægra stigi „síunar" ef það er yfirhöfuð mögulegt.

Ekki er að finna sérstakt ákvæði í lögum eða skilmálum netþjónustuaðilanna sem heimila fyrirtækjum að sía út póst með þeim hætti án heimildar frá móttakanda. Hins vegar verður ekki séð að unnt sé að taka á þessum vanda svo vel sé með öðru móti.

Nauðsynlegt er að sía ruslpóst til að tryggja virkni neta og slík síun sé liður í þjónustu við neytandann og í reynd flestum til hagsbóta þó að vefengja megi heimild netþjónustuaðila til þess að óbreyttu. Hæpið er að taka upp sérstök lagaákvæði sem kveði á um heimildir netþjónustuaðila til að henda pósti án heimildar frá móttakanda, eðlilegra er að slíkt sé hluti af samningi einstaklinga og fyrirtækja við netþjónustuaðilann.

Lagt er til að netþjónustuaðilar taki upp skýr ákvæði í skilmála sína sem heimila þeim síun ruslpósts með þeim hætti sem gert er þannig að heimildina sé að finna í samningi milli aðila.

3.6. Rafræn skilríki

Til þess að rafræn samskipti milli manna geti orðið almenn þarf að byggja upp kerfi sem nýtur trausts.

Traust er þeim mun nauðsynlegra í rafheimum þar sem samskiptaleiðir þar eru jafnan miklu síður áþreifanlegar. Móttakandi rafrænnar sendingar þarf að geta treyst því að:

- sendandi sé sá sem hann segist vera,
- það sem sent var hafi ekki breyst á leiðinni til móttakanda og
- sendandi geti ekki afneitað sendingum sínum,
- stundum er þörf fyrir dulritun texta og hindra þannig að óviðkomandi geti lesið það sem sent er.

Þá er vaxandi þörf fyrir að notandi rafrænnar þjónustu geti auðkennt sig tryggilega gagnvart kerfum þjónustuveitenda með traustverðum og sannanlegum hætti.

Þessum markmiðum má ná með því að nota rafræn skilríki byggð á svokölluðum ósamhverfum dulritunarlyklum. Kerfi aðferða og reglna til að tryggja formfestu og öryggi í útgáfu og meðferð slíkra skilríkja er kallað *dreifilyklaskipulag* (e. Public Key Infrastructure, PKI). Traust dreifilyklaskipulag byggist í raun að meira leyti á skipulagi og vinnubrögðum en á tækni.

Samkvæmt stefnu ríkisstjórnarinnar um upplýsingasamfélagið skal stefnt að því að notkun rafrænna skilríkja verði almenn og útbreidd hér á landi. Nauðsynlegt er að stjórnvöld vinni

[31] Sjá t.d.12. gr. í skilmálum Símans þar sem segir „Óheimilt er að nota aðganginn til fjöldasendinga, þ.m.t. að senda magnpóst sem ekki inniheldur réttar upplýsingar um sendanda. Óheimilt er að nota aðganginn til að taka við svörum við slíkum pósti". Í 7. gr. skilmála OgVodafone. segir Viðskiptavini er ekki heimilt að trufla, skerða eða á nokkurn hátt hafa áhrif á notkun annarra viðskiptavina, til dæmis með fjöldapóstsendingum. (skilmálar eins og þeir birtust á heimasíðum félaganna í desember 2005)

markvisst að því að útbreiða notkun rafrænna skilríkja og sýni frumkvæði eða leiti eftir samvinnu við atvinnulífið um leiðir til að ná því markmiði.

Almenn útbreiðsla rafrænna skilríkja felur í sér byltingu í samskiptum á netinu. Með þeim skapast traust þar sem notendur geta með öruggum hætti auðkennt sig gagnvart öðrum, skrifað rafrænt undir skjöl og skuldbindingar og aukið öryggi og leynd með dulritun. Samhliða almennri útbreiðslu má gera ráð fyrir að framboð á rafrænum þjónustum margfaldist sem mun skila sér í auknu hagræði fyrir þjónustuveitendur, fyrirtæki og almenning.

Nauðsynlegt er að stjórnvöld hafi frumkvæði að því að taka upp rafræn skilríki, þar sem við á, bæði í samskiptum sín á milli og við aðra.

Lagt er til að útbreiðsla rafrænna skilríkja og gerð dreifilyklaskipulags fyrir allt landið verði gerð að forgangsmáli stjórnvalda í samræmi við áður tilvitnaða stefnu ríkisstjórnarinnar.

Lagt er til að settar verði leiðbeinandi reglur um notkun rafrænna skilríkja hjá ráðuneytum og ríkisstofnunum þ.m.t.um dulritun mikilvægra skjala sem send eru í tölvupósti og öryggisstig upplýsinga.

3.7. Þátttaka í alþjóðlegu samstarfi

Rafræn samskipti eiga sér engin landamæri ekki frekar en þróun Internetsins. Barátta fyrir auknu öryggi í því umhverfi er því áskorun fyrir allar þjóðir. Líta verður á net- og upplýsingaöryggi sem vandamál sem ekki verður eingöngu tekist á við með aðgerðum hérlendis. Jafnframt verður að byggja á alþjóðlegu samstarfi á þessu sviði og Íslendingar verða að vera virkir þátttakendur í því samstarfi ef árangur á að nást. Þá er eftir meiru að sækjast á þessu sviði fyrir smærri ríki, sem hafa takmarkað bolmagn í baráttu við alþjóðlegan vanda. Samstarf á þessu sviði felst m.a. í upptöku og gerð staðla, stefnumótun og samvinnu um öryggismál og víðtæk upplýsingaskipti.

Í ljósi þeirrar skörunar, t.d. milli ráðuneyta og stofnana á sviði upplýsingasamfélagsins, er nauðsynlegt að bæta eða koma á formlegra samstarfi um miðlun upplýsinga sem máli skipta og tengjast hinu erlenda samstarfi. Jafnframt að þeir, sem fái tilboð um þátttöku í samstarfi, láti vita af því. Hugsanlega mætti miðla þessum upplýsingum í ríkara mæli gegnum póstlista eða setja á innra net ráðuneyta þegar það verður virkt eða sameiginlega UT-síðu.

Lagt er til að stefna stjórnvalda kveði á um virka þátttöku í erlendu samstarfi enda sé það mikilvæg leið til árangurs. Hvetja til samstarfsins og leggja áherslu á að þau miðli upplýsingum til annarra innlendra aðila.

3.8. CERT-skipulag, viðvörunarskipulag

CERT-hópar[32] eru oft kallaðir CSIRT-hópar (e. Computer Security Incident Response Teams). Um er að ræða hópa sem samræma viðbrögð við óvæntum atburðum er varða öryggi í netkerfum. Slíkir hópar geta bæði starfað á alþjóðlegum vettvangi og innan einstakra ríkja. Almennt gildir að hver hópur skilgreinir sín markmið og starf. Misjafnt er hvernig ríkin í kringum okkur standa að þessum málum. Sum þeirra hafa valið að ein stofnun/samtök fari með CERT-hlutverk fyrir viðkomandi ríki en í öðrum er um fleiri en einn aðila að ræða.[33]

Í CERT-hópnum eigi sæti þeir aðilar sem koma að rekstri netkerfa og aðilar frá stjórnsýslunni. Verkefni hópsins er m.a. að skilgreina sameiginlega hagsmuni og móta vinnureglur. Jafnframt

[32] Skrásett nafn Carnegie Mellon University, Pittsburg, USA. Starfsemin hófst í Carnegie Mellon 1998 en árið 2003 gerði „U.S. Department of Homeland Security“ samning við aðila þar um að starfrækja US-CERT hóp fyrir hönd USA (CERT/CC).

[33] Nefna má að fjölmörg rannsókna- og menntanet eru innan TERENA-samtakanna í Hollandi (http://www.terena.nl). Rhnet er þáttakandi í þessu samstarfi í fyrir hönd íslenskra háskóla og rannsóknarstofnana.

að fjalla um hvort raunhæft sé að tengja saman upplýsingar frá net- og upplýsingakerfunum á skipulegan hátt.

Koma verður á aðvörunarskipulagi sem hentar íslenskum aðstæðum og sem rekstraraðilar geta nýtt sér til að vernda netkerfi sín gegn ógnum sem steðja að net- og upplýsingaöryggi. Þetta skipulag nær til mikilvægra netkerfa opinberra stofnana og fyrirtækja sem gerir þeim kleift að bregðast sameiginlega og skjótt við með aðgerðum til að draga úr tjóni. Stjórnvöld bera ábyrgð á að koma skipulaginu á innan stjórnsýslunnar. En atvinnulífið og stjórnvöld verða hins vegar sameiginlega að taka ákvarðanir um útfærslu á fyrirkomulaginu sín á milli enda er þátttakan valkvæð.[34]

Aðkoma opinberra aðila að CERT-málum verði fólgin í yfirumsjón með því að aðilar sem veita netþjónustu sinni sameiginlegum öryggishagsmunum á skipulegan hátt. Samhæfa þarf viðbrögð þeirra rekstraraðila sem veita þjónustu við útlönd og koma boðum til CERT-aðila erlendis. Í heimsóknum starfshópsins til rekstraraðila kom í ljós skýr vilji fyrirtækjanna til að koma að þessum sameiginlegu hagsmunum.

Verkefni CERT-hóps verði að taka á tilkynningum um árásir eða tilraunir til árása á innviði netkerfa, sjálfvirkar árásir á vefsíður, grófar tilraunir til innbrota í fjarskiptanetið og þegar vart verður við nýjar aðferðir sem hafa áhrif á virkni net- og upplýsingakerfa. Starfssvið CERT getur m.a. verið fólgið í því að :

- leiðbeina og veita ráðgjöf og upplýsingar um hvernig hægt sé að bæta net- og upplýsingaöryggi,
- veita upplýsingar um hvernig koma megi í veg fyrir að atburðir, sem ógna net- og upplýsingaöryggi, eigi sér stað,
- starfa í samvinnu við innlenda þjónustuaðila netkerfa og hugbúnaðarframleiðendur,
- hafa samstarf við lögreglu og stjórnvöld,
- fylgjast með og greina alþjóðlega þróun á sviði net- og upplýsingaöryggis.
- vera í samvinnu við stjórnvöld annarra landa sem koma að CERT-málum.

Lagt er til að Póst- og fjarskiptastofnun hafi frumkvæði að því að koma á og skipuleggja CERT-samstarf við hagsmunaaðila. Eðlilegt er að stofnunin annist rekstur slíks samstarfs, leggi til nauðsynlega aðstöðu og sjái um samráð við aðrar stofnanir ríkisins.

3.9. Samhæfing varðandi net- og upplýsingaöryggi

Öryggismál eru vaxandi þáttur að umfangi í allri starfsemi sem fram fer í samfélaginu, hvort sem það leiðir af hættum vegna hryðjuverka eða af annarri brotastarfsemi og með kostnaði sem af þeim leiðir. Þrátt fyrir að net- og upplýsingaöryggi falli undir verksvið og sé á ábyrgð stjórnvalda er það í reynd hvers og eins, einstaklinga eða lögaðila, að gæta að eigin öryggi á þessu sviði. Eðlilegt er að stjórnvöld komi á samhæfingu og eftirliti með framkvæmd á þessu sviði. Skort hefur á markvissa og samhæfða framkvæmd.

Nauðsynlegt er að samhæfa aðgerðir stjórnvalda varðandi net- og upplýsinga-öryggi, samgöngu- og veitukerfa og almannaþjónustu, m.a. með tilliti til þjóðaröryggissjónarmiða.

Eins og vikið hefur verið að hér að framan er samgöngu- og veitukerfum og almannaþjónustu samfélagsins, þ.e. orka, vatn, flug-, skipa- og landflutningar, heilsuvernd, löggæsla, banka- og verðbréfaþjónusta, neyðarþjónusta (112) að verulegu leyti stjórnað með samskipta eða fjarskiptanetum. Ábyrgð og öryggi þeirra hvílir á viðkomandi rekstraraðilum sem eru eftir atvikum fyrirtæki, stofnanir eða stjórnvöld, sjá töflu. Vegna mikilvægis kerfanna fyrir samfélagið allt verður að huga sérstaklega að virkni þeirra við óvenjulegar eða sérstakar aðstæður eins og t.d. náttúruhamfarir, skemmdarverk eða önnur áföll sem geta leitt til alvarlegrar röskunar á starfsemi þeirra, eins eða fleiri, eða í röskun á starfsemi annarra kerfa.

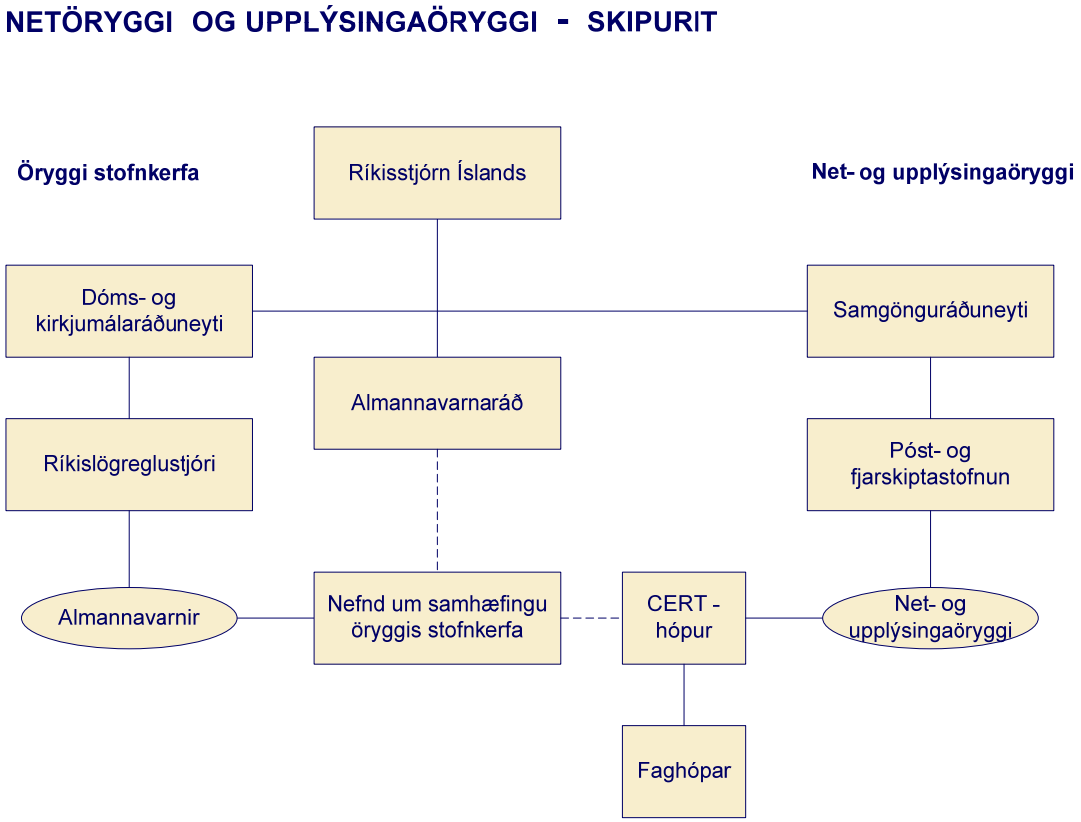
[34] Benda má á að ENISA-stofnunin mun veita ráðgjöf varðandi útfærslu á CERT-starfsemi og að eitt aðaláherslumál ESB er að efla og samhæfa CERT-hópa innan ESB, sem og að efla alþjóðlega samvinnu.

Tegund nets og hlutverk	Samhæfing og eftirfylgni á kröfum til upplýsingatækni	Skilgreina kröfur til netkerfa og fylgja þeim eftir	Innleiða kröfur til netkerfa
Fjarskipti	Samgönguráðuneyti	Póst- og fjarskiptastofnun	Fjarskiptafyrirtæki netþjónustuaðilar
Fjármálastarfsemi	Viðskiptaráðuneyti	Fjármálaeftirlit	Seðlabankinn og bankastofnanir
Orkuveita	Iðnaðarráðuneyti	Orkustofnun	Landsvirkjun Landsnet hf. veitustofnanir
Vatnsveita	Félagsmálaráðuneyti	Sveitarfélög	Veitustofnanir sveitarfélaga
Eldsneyti	Iðnaðar- og viðskiptaráðuneyti	Orkustofnun	Olíufélögin
Flutningastarfsemi	Samgönguráðuneyti	Flugmálastjórn Vegagerðin Siglingastofnun	Flutningafyrirtæki
Heilbrigðisþjónusta	Heilbrigðis- og tryggingaráðuneyti	Landlæknisembættið	Heilbrigðisstofnanir
Neyðarþjónusta	Dóms- og kirkjumálaráðuneyti	Ríkislögreglustjórinn lögregluembætti, slökkvilið og sjúkraflutningar	Neyðarlínan hf., Sveitarfélög
Löggæsla	Dóms- og kirkjumálaráðuneyti	Ríkislögreglustjórinn Landhelgisgæslan	Lögregluembætti
Almannavarnir	Dóms- og kirkjumálaráðuneyti	Ríkislögreglustjórinn Almannavarnaráð Vísindasamfélagið	Landhelgisgæslan lögregluembætti
Stjórnsýsla ríkisins	Forsætisráðuneyti	Önnur ráðuneyti og ríkisstofnanir	Ríkislögreglustjórinn

Tafla 5. Innan íslenskrar stjórnsýslu eru það eftirtalin ráðuneyti og stofnanir sem bera ábyrgð á helstu þáttum sem geta varðað öryggi viðkomandi net- og upplýsingakerfa. Mikilvægt er að kortleggja hvernig einstaka þættir geta haft áhrif hver á annan.

Lagt er til að komið verði á fót sérstakri nefnd, sem skipuð yrði fulltrúum stjórnsýslunnar og rekstraraðila, til að huga að netöryggi og samhæfingu vegna áðurnefndra kerfa. Nefndin þarf að hafa einhver formleg tengsl við almannavarnir eða Almannavarnaráð. Einnig er mikilvægt að hún hafi samstarf við CERT-hóp sbr. nánari umfjöllun í kafla 3.8.

Í 1. gr. laga nr. 94/1962 um almannavarnir er fjallað um hlutverk almannavarna sem felst í því að koma í veg fyrir, eftir því sem unnt er, að almenningur verði fyrir líkamstjóni eða eignatjóni vegna tiltekinna atburða og að veita aðstoð vegna tjóns o.s.frv. Þá er í 6. gr. kveðið á um hlutverk ríkislögreglustjóra og ráðgjafarhlutverk Almannavarnaráðs. Ekki verður séð að lögin nái að óbreyttu til samhæfingar í þeirri merkingu sem hér hefur verið rætt um þó að eðlilegt sé að svo væri. Taka þarf til athugunar í þessu sambandi hvort ekki sé kominn tími til að endurskoða í heild lög nr. 94/1962 um almannavarnir. Virðast þau vera heldur fátækleg varðandi þær hættur sem nútímasamfélög standa frammi fyrir, t.d. hvað varðar öryggi fjarskipta- og orkukerfa. Er það mat hópsins að kveða þurfi nánar á um ábyrgð á rannsóknum, áhættugreiningu, gerð viðbragðsáætlana o.fl. í tengslum við þær hættur sem eru til umfjöllunar í skýrslu þessari.



Skipuritið hér fyrir ofan sýnir skipulag net- og upplýsingaöryggis í samræmi við tillöguna í skýrslunni. Samræming og eftirlit með öryggi hina ýmsu veitukerfa sbr. Tafla 5, og virkni þeirra út frá þjóðaröryggissjónarmiðum yrði verkefni nefndar sem félli undir almannavarnir. CERT starfsemi yrði verkefni sem yrði hluti af net- og upplýsingaöryggis starfsemi Póst- og fjarskiptastofnunar.

Þá er ennfremur þörf á samræmingu á afmarkaðri sviðum net- og upplýsingaöryggis, t.d. varðandi:

- upplýsingagjöf og hleranir fjarskiptakerfa í tengslum við rannsóknir lögreglu,
- samræmd viðbrögð við árásum á net- og upplýsingakerfi, t.d. ef loka þarf fyrir umferð,
- skipulag vegna þarfa ríkisins fyrir fjarskipti vegna náttúruhamfara eða annarrar utanaðkomandi röskunar og einnig samstarf milli fjarskiptafyrirtækja við þær kringumstæður,[35]
- sérstakar þarfir stjórnsýslunnar.

Rétt þykir að samræming sem þessi fari fram í mismunandi faghópum sem hafi tengsl við eða falli undir CERT-starf.

3.10. Öryggi - tenging við umheiminn

Stærsti einstaki veikleiki í öryggi landsins varðandi upplýsinga- og fjarskiptatækni eru tengingar við útlönd. Eins og er eru tvær tengingar við landið. Annars vegar um Canntat3 sem er elsti sæstrengur í notkun á N-Atlantshafi með takmarkaða flutningsgetu og byggir á úreltri tækni. Hins vegar er Farice1 sem byggir á nýrri tækni með flutningsgetu til næstu framtíðar, en hann er ekki hringtengdur þannig að rof á einum stað rýfur gagnaflutning um strenginn. Endurteknar bilanir á Farice1 sambandinu hafa valdið nokkrum truflunum, en allar bilanir hingað til hafa verið á landi. Þegar hefur verið bætt úr þessu að hluta með tvöföldun strengsins nyrst í Skotlandi. Verulegt áhyggjuefni er ef bilun yrði á strengnum í sjó þar sem viðgerð getur

[35] Huga þarf t.d. að útfærslu á ákvæðum 2. mgr. 6. gr. og að 72. gr. fjarskiptalaga varðandi nauðsyn þess að tryggja fjarskipti milli björgunarsveita og yfirvalda og útvarpssendingar til almennings þegar stórslys og hamfarir verða og að 72. gr. varðandi stöðvun fjarskipta.

tekið allt að 14 daga. Þar að auki er nú búið að taka Skyggni niður en hann þjónaði sem aðal varasamband landsins um gervihnött (Intelsat).

Verulegir öryggis- og viðskiptahagsmunir eru bundnir við millilandasambandið og alvarleg röskun á því getur haft alvarlegar afleiðingar fyrir allt samfélagið.[36]

Þá er verðlagning á millilandasamböndum hátt í erlendum samanburði og hindrun í þróun fjarskiptamarkaðarins sem getur hrakið hugbúnaðarfyrirtæki og þjónustuaðila úr landi.[37] Hýsing alþjóðlegra tölvuvera hérlendis er álitin ólíkleg þrátt fyrir hagstætt orkuverð (mikla orkunotkun þarf til kælingar) vegna verðlagningar á millilandasamböndum og ótryggs sambands við landið.

Bent er á að stjórnvöld hafa þegar mótað ákveðna stefnu í þessum málum, annars vegar í stefnu ríkisstjórnarinnar varðandi upplýsingasamfélagið *Auðlindir í allra þágu*[38] og í fjarskiptaáætlun fyrir árin 2005–2010 sem samþykkt var á Alþingi í 11. maí s.l.[39] um að tryggja beri fullnægjandi varasambönd.

Leggja verður áherslu á það grundvallarsjónarmið varðandi ábyrgð stjórnvalda í öryggismálum, að tryggja þá þætti er varða öryggi alls samfélagsins. Öryggi og tilvist millilandasambanda er af þeim toga. Ekki verður séð að stjórnvöld komist hjá því að koma að þessum málum enda er ekki hægt að gera ráð fyrir samkeppni á þessu sviði. Burðargeta Farice1-strengsins er nægjanleg fyrir næstu framtíð þannig að annar sæstrengur verður fyrst og fremst lagður til að auka rekstraröryggi fyrirtækja og einstaklinga á Íslandi.

Lagt er til að stjórnvöld tryggi fjármögnun nýs fjarskiptastrengs sem yrði varasamband landsins við útlönd. Jafnframt verði hugað að verðlagningu og hugsanlega rekstrarformi sæstrengja sem stjórnvöld taka þátt í að fjármagna.

Þá skiptir máli að við lagningu nýs strengs sé ekki bara horft til hagsmuna símafyrirtækja, einnig verður að hafa í huga þarfir annarra fyrirtækja t.d. á sviði hugbúnaðar, þjónustu og viðskipta.

3.11. Breytingar og samræming á löggjöf

Skýr og greinargóð löggjöf er tekur til net- og upplýsingaöryggis er forsenda þess að unnt sé, með skilvirkum hætti, að koma í veg fyrir og bregðast við hugsanlegum áföllum í rekstri fjarskiptaneta. Notendur fjarskiptaþjónustu verða að eiga kost á einföldum lausnum til að þess að gæta að einkalífsvernd sinni og öryggi í fjarskiptum. Tryggja þarf að til staðar séu nauðsynleg lagaleg úrræði til að bregðast við kvörtunum frá notendum í þessu sambandi. Þá þurfa stjórnvöld sem starfa á þessu málefnasviði og sérfræðingar sem koma að reglugerðarvinnu, að skiptast á skoðunum og útfæra sameiginlegar aðferðir þannig að þeir

---

[36] Benda má t.d. á einfalda hluti eins og að öll skráning flugfarþega er rafræn. Nauðsynleg upplýsingaskipti á farþegalistum eru jafnframt að verða forsenda vegna flugs til annarra landa (BNA) og þau eru rafræn. Verðbréfa- og bankaviðskipti hér eru alþjóðleg og byggja á millilandatengingum.

[37] Virt fyrirtæki á þessu sviði Friðrik Skúlason hf. (FRISK) reiðir sig mikið á millilandatengingar, m.a. vegna uppfærslu á hugbúnaði sem það selur um allan heim. Fyrirtækið bendir á að verðlag hér sé 8-11 sinnum dýrara en erlendis.

[38] Þar segir: „Sett verði öryggisviðmið vegna reksturs almennra fjarskiptaneta á Íslandi og vegna tenginga Íslands við umheiminn, m.a. með það að leiðarljósi að tryggja öryggi fjarskiptasambanda bæði innanlands og milli Íslands og annarra landa. Gerð verði sú lágmarkskrafa að ávallt verði tveir sæstrengir tengdir við landið auk varasambanda um gervihnött".

[39] Þar segir: „Öryggi almennra fjarskiptaneta innanlands og við umheiminn verði tryggt með fullnægjandi varasamböndum. Að gert verði áhættumat um tengingu Íslands við útlönd og tryggt að öryggismálum verði þannig háttað að tenging rofni ekki. Lágmarksþjónusta og viðbragðsáætlun verði skilgreind ef bregðast þarf við bilun eða ógn, t.d. ef tenging gegnum sæstreng rofnar". Þá er kveðið á um það í 2. mgr. 2. fjarskiptalaga sem fjallar um gerð fjarskiptaáætlunar að með henni eigi m.a. *tryggja öryggi tengingar Íslands við umheiminn* (f-liður).

fjármunir sem notaðir eru til þessa málaflokks nýtist betur, samskipti við stjórnvöld verði einfaldari og atvinnulífið verði fyrir minna álagi.

3.11.1. Reglur um öryggi og viðbúnað

Í þeim tilgangi að tryggja sem best net- og upplýsingaöryggi er nauðsynlegt að fjarskiptafyrirtæki setji sér öryggisstefnu, framkvæmi áhættugreiningu og skjalfesti þær öryggisráðstafanir sem gripið er til á grundvelli slíkrar greiningar. Telja verður eðlilegt að slík vinna taki mið af staðlinum um stjórnun upplýsingaöryggis, sbr. umfjöllun í kafla 3.2.

Samkvæmt 1. mgr. 47. gr. fjarskiptalaga skulu fjarskiptafyrirtæki gera viðeigandi ráðstafanir til að tryggja öryggi fjarskiptaþjónustu. Í lögin skortir hins vegar sérstök ákvæði um net- og upplýsingaöryggi. Að mati starfshópsins er mikilvægt að skilgreina andlag net- og upplýsingaöryggis og útfæra nánar þær kröfur um viðbúnað sem fjarskiptafyrirtækjum ber að viðhafa. Á þetta ekki síst við um þær tæknilegu ráðstafanir sem stuðla eiga að samfelldum rekstri fjarskiptaneta.

Leggur nefndin því til að í fjarskiptalög verði sett ákvæði er mæli fyrir um skyldu fjarskiptafyrirtækja til að skjalfesta hvernig staðið er að net- og upplýsingaöryggi. Enn fremur að á grundvelli slíks ákvæðis verði Póst- og fjarskiptastofnun falið að setja nánari reglur um öryggi og viðbúnað í almennum fjarskiptanetum. Mikilvægt er að slíkar reglur taki ekki eingöngu til fjarskiptafyrirtækja heldur til allra aðila sem veita internetþjónustu og einnig til starfsemi hýsingaraðila.

3.11.2. Tölvuglæpir

Internetið er í vaxandi mæli orðinn vettvangur verslunar og viðskipta og er því brýnt að löggjöfin endurspegli þessa þróun. Með lögum nr. 30/1998 um breytingu á almennum hegningarlögum nr. 19/1940 voru refsiheimildir endurskoðaðar með það fyrir augum að ná til s.k. tölvuglæpa, þ.e. afbrota sem framin er með því að nota tölvu, eða sem beinast að tölvum, hugbúnaði (forritum) eða gögnum og upplýsingum sem varðveittar eru í tölvum eða á tölvutæku formi. Hins vegar hefur enn sem komið er ekki mikið reynt á þessi ákvæði.

Að sama skapi er mikilvægt að í lögum sé kveðið á um nauðsynleg rannsóknarúrræði til handa lögreglu til að upplýsa og rannsaka tölvuglæpi. Á vegum dómsmálaráðuneytisins var unnið að að nauðsynlegum lagabreytingum vegna fullgildingar Íslands á samningi Evrópuráðsins um netglæpi[40] (Convention on Cybercrime) frá 23. nóvember 2001. Alþingi samþykkti þessar breytingar með lögum nr. 74/2006 sem fela í sér að nýju ákvæði var bætt inn í lög nr. 19/1991, um meðferð opinberra mála, sem heimilar lögreglu, í þágu rannsóknar opinbers máls, að leggja fyrir þann sem rekur fjarskiptaþjónustu eða fjarskiptanet að varðveita tölvugögn, án þess að afla þurfi undanfarandi dómsúrskurðar. Þá voru rýmkuð nokkuð skilyrði fyrir því að lögregla geti aflað dómsúrskurðar í slíkum málum. Umræddar breytingar kölluðu jafnframt á breytingar á hegningalögum og fjarskiptalögum[41].

Til að tryggja öryggi fjarskipta og friðhelgi einkalífs þurfa fjarskiptalög að sjá fyrir hugsanlega misnotkun á fjarskiptabúnaði. Við athugun hefur komið í ljós að í fjarskiptalögin skortir ákvæði er bannar að með ólögmætum hætti sé komið fyrir hugbúnaði í endabúnaði notenda. Er hér átt við svokallaðan njósnahugbúnað (e. spyware), vefhlerunarhugbúnað (e. web bugs) og annan svipaðan búnað sem unnt er að koma fyrir í endabúnaði notanda án vitundar hans, til þess að fá aðgang að upplýsingum, safna földum upplýsingum eða fylgjast með athöfnum notandans og getur með alvarlegum hætti rofið friðhelgi einkalífs hans. Hins vegar getur slíkur búnaður, t.d. smygildi (e. cookies), verið lögmætt og nytsamlegt tól, t.d. til að greina skilvirkni vefsetursbönnunar og auglýsinga og við að sannprófa kenni notenda sem eiga beintengd

[40] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[41] Lög nr. 74 14. júní 2006 um breyting á almennum hegningarlögum, lögum um meðferð opinberra mála og lögum um fjarskipti (samningur Evrópuráðsins um tölvubrot).

viðskipti. Lagt er til að tekið verði upp í fjarskiptalög ákvæði er banni að með ólögmætum hætti sé komið fyrir hugbúnaði í endabúnaði notenda.

Í erlendum samanburði hefur komið í ljós að notkun eldveggja meðal almennings hér á landi er mun minni en á hinum Norðurlöndunum en þeir eru, eins og fram hefur komið, mikilvægir í vörnum tölva.[42]

Lagt er til að þjónustuaðilar og samtök sem starfa á þessu sviði hvetji til notkunar eldveggja eða annars varnarbúnaðar og að í kynningarefni um þessi mál verði lögð áhersla á þennan þátt.

3.12. Verkaskipting eftirlitsaðila

Við skoðun á þeim álitaefnum er varða net- og upplýsingaöryggi kemur fljótt í ljós að töluverð skörun er í málaflokknum milli ráðuneyta og stofnana. Þetta kemur skýrast fram í skipun starfshópsins sem samanstendur af fulltrúum sjö ráðuneyta og þriggja stofnana sem hafa með einum eða öðrum hætti með þessi mál að gera. Taflan hér fyrir neðan sýnir m.a. þessa skörun þegar kemur að eftirliti og að sinna erindum eða kvörtunum almennings. Í sumum tilvikum getur álitaefnið heyrt undir tvo eða þrjá eftirlitsaðila. Í mörgum tilvikum getur verið tilefni til kæru til lögreglu án þess að það sé nokkur von til þess að slík kæra skili árangri t.d. vegna veirusendinga, ólögmæts aðgangs eða ruslpósts þar sem sendandinn er oftast erlendur og/eða óþekktur. Eðlilegt er að til sé farvegur fyrir erindi og kvartanir sem þessar og að hægt sé að aðstoða, veita upplýsingar eða leiðbeina þ.m.t. um aðgerðir til að hindra endurtekningu eða vegna frekari gagnaöflunar til áframhaldandi kærumeðferðar t.d. til lögreglu. Leysa mætti stóran hluta af þessu með aðgengilegum upplýsingum á Internetinu t.d. á heimasíðu um öryggismál. Mikilvægt er í þessu sambandi að fyrir liggi skýr skil milli ábyrgðar og hlutverks hvers eftirlitsaðila þannig að ekki sé vafi um til hvers almenningur eigi að snúa sér með erindi og kvartanir. Brugðist hefur verið við þeim vanda sem fellst í skörun í eftirliti m.a. með tillögum til lagabreytinga í 4. kafla.

Þrátt fyrir tillögur sem miða að því að skýrðar séu markalínurnar milli eftirlitsaðilanna er ekki þar með sagt að öll vandamál í þessu sambandi hafi verið skýrð. Ef skil eru ekki skýr er það skv. stjórnsýslulögum, eftirlitsaðilanna að leysa úr þeim vanda en ekki borgaranna.

[42] Sjá Nordic Information Society Statistics 2005, TemaNord 2005:562.

Eftirlits- eða ábyrgðaraðilar

	Opinberir aðilar			Þjónustuaðilar/félagasamtök			
Tegund erindis/kvörtunar	Póst- og fjarskiptastofnun	Persónuvernd	Ríkislögreglustjóri	Fjarskiptafyrirtæki	Netþjónustuaðilar	Barnaheill	Heimili og skóli
Inngrip í fjarskiptasendingar	X▲		X*	X	X		
Ólögmætur aðgangur að persónuupplýsingum		X▲	X				
Ólögmætur aðgangur að netkerfum	X▲		X	X			
Vefveiðar (phishing)		X	X▲				
Truflun á virkni netkerfa	X▲		X**	X	X		
Skaðlegur hugbúnaðar (veirur)	X▲		X**		X		
Fölsun á uppruna sendinga			X▲		X		
Ruslpóstur (spam)	X▲	X	X**		X		
Markpóstur með tölvupósti, síma, faxi, sjálvirku uppkallskerfi	X▲	X	X				
Markpóstur í bréfpósti	X▲	X	X				
Skaðlegt innihald			X▲			X	X
Klám (börn)			X▲			X	X

*Ásetningur og stórkostlegt gáleysi
** Ef um er að ræða tjón

TAFLA 3, sýnir með X yfirlit yfir aðila sem almenningur getur í dag leitað til með erindi eða kvartanir vegna atriða er varða net- og upplýsingaöryggi eða önnur siðferðisleg álitaefni tengda Internetinu. Táknið ▲ sýnir þá opinberu aðila sem almenningur getur leitað til með umkvörtunarefni í samræmi við tillögur um lagabreytingar. Hafa ber í huga að valdheimildir þeirra eru með ólíkum hætti.

Eins og áður sagði er mikilvægt að upplýsingar og leiðbeiningar um öryggismál séu almenningi aðgengilegar á Internetinu. En það mætti einfalda þetta enn frekar með því að koma upp vefsíðu með leiðbeiningum varðandi öll erindi eða kvartanir á þessu sviði burtséð frá því hver ber ábyrgð á úrlausnarefninu. Markmiðið væri að auðvelda almenningi að koma erindum sínum á framfæri við réttan aðila með einföldum hætti. Hugsanlega gæti þetta verið þjónusta á vef um öryggismál (www.netoryggi.is) sem tengdist stjórnaráðsvef eða www.island.is. Eftirlitsstofnanirnar, Persónuvernd, Póst- og fjarskiptastofnun og Ríkislögreglustjórinn yrðu að koma sér saman um slíkar leiðbeiningar.

Fræðsla um net- og upplýsingaöryggi fellst m.a í upplýsingum til almennings um hvert hann geti snúið sér með umkvartanir sínar á þessu sviði.

3.13. Samþætting upplýsingatækni, fjarskipta og fjölmiðlunar

Í stafrænu umhverfi er sjónvarpsdagskrá í raun eins og hver annar gagnaflutningur og því er ekkert því til fyrirstöðu að fjölmiðlafyrirtæki sendi efni sitt um Internetið á svonefndum IP-staðli. Sá staðall er notaður er fyrir ýmiss konar gagnaflutning en símaþjónusta er í auknum mæli að flytjast yfir á hann (e. Voice-over-IP). Um IP-staðalinn gilda ekki sambærilegar reglur þar sem sömu kvaðir hafa ekki verið settar á Internetið og ljósvakamiðla. Í stafrænu umhverfi er erfitt að gera greinarmun á þessu tvennu.

Um heimildir til útvarps- og sjónvarpsrekstrar gilda ákvæði útvarpslaga, nr. 53/2000 en málaflokkurinn heyrir undir menntamálaráðuneytið. Útvarpsréttarnefnd veitir útvarpsleyfi til útvarps- og sjónvarpsfyrirtækja en Póst- og fjarskiptastofnun veitir tíðnileyfi í samræmi við ákvæði laga um fjarskipti nr. 81/2003. Útvarps- og sjónvarpsrekstur sem fram fer í gegnum dreifiveitur sem styðjast við IP-staðalinn, t.d. ADSL, virðist ekki falla undir útvarpslögin og eftirlit útvarpsréttarnefndar. Eftir sem áður gilda um hann almenn ákvæði fjarskiptalaga. Samkvæmt þeim gilda ákveðnar reglur um endabúnað notenda, kvaðir um opinn aðgang, skyldu til að flytja útvarpsdagskrá, skilyrt aðgangskerfi, staðla í gagnvirkri sjónvarpsþjónustu o.fl. Þannig virðast gilda mismunandi reglur og kröfur um fjölmiðlun eftir því hvaða tækni stuðst er við. Dæmi um þetta er Skjárinn, sem þarf af framangreindum ástæðum ekki útvarpsleyfi og er eingöngu háð eftirliti Póst- og fjarskiptastofnunar á grundvelli fjarskiptalaga.

Vegna tækniþróunar í fjölmiðlun hefur skapast grundvöllur til rekstrar fjölmiðla sem lögsaga íslenskra stjórnvalda nær ekki yfir. Með samruna fjölmiðla-, fjarskipta- og tölvutækni er ekkert því til fyrirstöðu að erlend fyrirtæki séu með fjölmiðlarekstur hér í gegnum netið. Með tilliti til þess að mismunandi er eftir ríkjum hvaða reglur gilda um fjölmiðlun, t.d. varðandi auglýsingar og textun efnis, er mikilvægt að hafa alþjóðlegt samstarf um reglur og eftirlit. Nú þegar er Póst- og fjarskiptastofnun í umtalsverðu alþjóðlegu samstarfi á sviði fjarskipta og upplýsingatækni.

Í ljósi samruna útvarps- og fjarskiptatækni er eðlilegt að einn aðili hafi með höndum leyfisveitingar, úthlutun fjarskiptatíðna og eftirlit með fjarskipta- og fjölmiðlastarfsemi óháð þeirri tækni sem liggur til grundvallar starfseminni.

4. Markpóstur og bein markaðssetning

Notendur fjarskiptaþjónustu eiga rétt á því að njóta verndar gegn því að númer þeirra og vistföng séu notuð gegn vilja þeirra í tengslum við markaðssetningarstarfsemi. Í gildandi lögum er að finna ákvæði í þremur lagabálkum sem taka á þessu, n.t.t. er um að ræða 14. gr. laga nr. 46/2000 um húsgöngu og fjarsölusamninga, 28. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga og 46. gr. fjarskiptalaga nr. 81/2003. Að efni til eru þessi ákvæði í nokkru ósamræmi hvort við annað, auk þess sem þrjú mismunandi stjórnvöld hafa eftirlit með því að þeim sé framfylgt, þ.e. Póst- og fjarskiptastofnun, Persónuvernd og viðskiptaráðuneytið. Af þessu leiðir að nokkur óvissa ríkir um það hvaða reglur gilda í þessum efnum og til hvaða stjórnvalds neytendum ber að beina kvörtunum sínum telji þeir á sér brotið.

Meðal þess sem veldur vandkvæðum vegna ósamræmis umræddra lagaákvæða er að reglur þeirra um beina markaðssetningu byggja á mismunandi aðferðarfræði. Annars vegar er um að ræða s.k. *samþykkisreglu* (opt-in), sem felur í sér að óheimilt er að stunda beina markaðssetningu gagnvart tilteknum aðila nema að samþykki hans sé fengið fyrir fram, sbr. 1. mgr. 46. fjarskiptalaga og 1. mgr. 14. gr. laga um húsgöngu og fjarsölu, og hins vegar s.k. *bannskrárreglu* (opt-out), sem felur það í sér að bein markaðssetning er óheimil gagnvart þeim aðilum sem óskað hafa eftir því að vera lausir við hana með því að skrá sig á sérstaka bannskrá þar að lútandi, sbr. 2. mgr. 28. gr. persónuverndarlaganna. Ef þessar tvær reglur taka til sama tilviks er ljóst að þær ganga í berhögg við hvor aðra.

4.1. Notkun venjulegs pósts

Ákvæði 14. gr. laga um húsgöngu og fjarsölusamninga og 46. gr. fjarskiptalaga gilda þegar um er að ræða notkun símbréfa, sjálfvirkra uppkallskerfa og tölvupósts við beina markaðssetningu en þau ná hins vegar ekki til hefðbundins pósts, skv. skilgreiningu 4. gr. laga nr. 19/2002 um póstþjónustu. Ákvæði 28. gr. persónuverndarlaganna taka hins vegar til markpósts óháð þeirri tækni sem notuð er til að koma honum á framfæri.

4.2. Notkun tölvupósts og sjálfvirkra uppkallskerfa

Þegar um er að ræða notkun tölvupósts við beina markaðssetningu er það túlkunaratriði hvort ákvæði fjarskiptalaga eða persónuverndarlaga hafi forgang. Ef einstaklingur er ekki skráður í bannskrá virðist engu að síður vera óheimilt að senda honum markpóst með tölvupósti, sbr. 1. mgr. 46. fjarskiptalaga (opt-in). Heimild 2. mgr. 28. gr. persónuverndarlaga til þess að senda einstaklingi markpóst, sem ekki er skráður í bannskrá, hefur þá enga þýðingu (opt-out). Sé einstaklingur aftur á móti skráður í bannskrá er óvíst hvort að heimild fyrirtækja til að senda eigin viðskiptamönnum markpóst samkvæmt undanþágu í 2. mgr. 46. gr. fjarskiptalaga eigi við.[43] Þess má geta að sambærilegt ákvæði í 3. mgr. 14. gr. húsgöngu og fjarsölulaganna áskilur ekki að um sé að ræða kynningu fyrirtækis á eigin vörum og þjónustu til viðskiptamanna sinna. Felur ákvæðið þannig í sér víðtækari undanþágu frá samþykkisreglunni en gert er ráð fyrir í fjarskiptalögum. Þess má geta að ekki virðist ljóst hvort samþykkisregla 1. mgr. 46. gr. fjarskiptalaganna taki til smáskilaboða (SMS). Kveða þarf á um það með skýrum hætti

4.3. Notkun síma

Varðandi símtöl er í fjarskiptalögum stuðst við bannskrárreglu, sbr. 2. mgr. 45. gr. og 5. mgr. 46. gr., þ.e. bannmerkingar í símaskrá. Vísað er til þessara ákvæða í 3. mgr. 14. gr. laga um húsgöngu og fjarsölusamninga. Þótt augljóst óhagræði sé af því að hafa bannmerkingar við símanúmer í fleiri en einni skrá eru ákvæði fjarskiptalaga að þessu leyti ekki í andstöðu við ákvæði 2. mgr. 28. gr. persónuverndarlaga, sem fjallar um bannmerkingar í bannskrá Hagstofu Íslands (nú Þjóðskrá). Rétt er að vekja athygli á að samkvæmt 5. mgr. 46. gr. fjarskiptalaga virðist bannskrárregla fjarskiptalaga ekki ná til þess að nota farsíma við beina markaðssetningu, sbr. orðalagið: „Notendur sem nota *almenna talsímaþjónustu...*," en samkvæmt orðskýringu í 2. tl. 3. gr. fjarskiptalaga merkir það: „Þjónusta opin almenningi sem miðlar innlendum og alþjóðlegum símtölum um *notendabúnað sem er tengdur föstum nettengipunkti*." Ekki er að finna þrengingu að þessu leyti í 2. mgr. 28. gr. persónuverndarlaga.

Þá má benda á að eins og málum er háttað í dag þurfa auglýsendur að uppfylla skilyrði núgildandi ákvæðis 5. mgr. 46. gr. fjarskiptalaga með því að afla sér upplýsinga um bannmerkt símanúmer úr prentaðri útgáfu símaskrár eða rafrænni útgáfu hennar. Já hf. annast nú útgáfu prentaðrar símaskrár og rekstur upplýsingaveitu um öll símanúmer en þetta er ein af þeim alþjónustukvöðum sem hvíla á Símanum hf. í dag. Ef um er að ræða mikinn fjölda símanúmera hefur verið vænlegast fyrir auglýsendur að kaupa samkeyrslu slíkra úthringilista við gagnagrunn símaskrár. Í þessu sambandi verður að teljast umdeilanlegt að kaupa þurfi þjónustu af tilteknu einkafyrirtæki til þess að uppfylla skilyrði í lögum. Þá ber að líta til þess að vernd gegn ónæði af völdum markaðsetningu í gegnum síma er einnig að finna í 2. mgr. 28. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Þar segir m.a. að óheimilt sé að nota skrá með símanúmerum í þágu beinnar markaðssóknar nema að bera hana áður saman við bannskrá Þjóðskrár til að koma í veg fyrir að hringt sé í einstaklinga sem hafa andmælt slíku. Hins vegar hefur Þjóðskrá ekki búið yfir upplýsingum um símanúmer landsmanna. Hefur því í reynd ekki verið nóg fyrir auglýsendur að bera úthringilista saman við bannmerkingar í símaskrá heldur hafa þeir einnig þurft að bera þá saman við bannskrá Þjóðskrár. Hefur þetta valdið auglýsendum talsverðu óhagræði og auknum kostnaði sem felst í því að kaupa samkeyrslur af tveimur aðilum. Einnig hefur þetta fyrirkomulag haft í för með sér óhagræði fyrir einstaklinga sem hafa þurft að setja sig í samband við tvo aðila til þess að öðlast virka vernd gegn ónæði af völdum markaðsetningar í gegnum síma.

4.4. Leiðir til úrbóta og tillögur að lagabreytingum

Að mati nefndarinnar þarf að grípa til aðgerða til að greiða úr þeirri réttaróvissu sem lýst hefur verið hér að framan. Annars vegar verður að upplýsa neytendur betur um hvert þeir eigi að

[43] Ef til samanburðar er litið til 3. mgr. 14. gr. laga um húsgöngu og fjarsölusamninga virðist vera óheimilt að senda tölvupóst undir þeim kringumstæðum, sbr. orðalagið: „Hafi neytandi ekki tilkynnt sig til skrár Hagstofu Íslands...og seljandi sendir honum í beinni markaðssókn tölvupóst..."

snúa sér vegna kvartana um ónæði af völdum markaðssetningar og gera þeim auðveldara að koma slíkum kvörtunum á framfæri við hlutaðeigandi stjórnvöld. Til dæmis kemur til greina að koma upp sérstakri þjónustusíðu þar sem hægt væri að taka við kvörtunum frá neytendum og koma þeim áfram á réttan áfangastað til úrlausnar (sbr. umfjöllun í kafla 3.3.). Hins vegar verður ekki hjá því komist að breyta lögum til að einfalda og samræma þau lagaákvæði sem lúta að beinni markaðssetningu.

Hægt er að fara ýmsar leiðir við samræmingu umræddra ákvæða. Helst kemur til greina að afmarka með skýrari hætti gildissvið þeirra með því að gera greinarmun á þeirri tækni sem notuð er við beina markaðssetningu en hrófla sem minnst við efni laganna að öðru leyti. Hefur sú leið þá kosti í för með sér að forræði yfir túlkun og framkvæmd umræddra ákvæða verður áfram hjá þeim stofnunum sem tilskipanir Evrópusambandsins (nr. 95/46/EB og nr. 2002/58/EB) gera ráð fyrir að fari með slíkt hlutverk, þ.e. hjá Persónuvernd og Póst- og fjarskiptastofnun. Hins vegar mætti horfa til hagsmuna neytenda af því að geta leitað til einnar stofnunar með kvartanir vegna markaðssetningar burtséð frá tækninni sem stuðst er við. Lagt er til að síðarnefndu sjónarmiðin ráði.

Þegar um er að ræða markaðssetningu þar sem stuðst er við póst- eða fjarskiptaþjónustu þykir eðlilegt að ákvæði þessa efnis sé að finna í viðkomandi sérlögum og þar sé kveðið á um skyldu til samkeyrslu við bannskrá Þjóðskrár. Þar sem ábyrgð með framvæmd þessara laga og eftirlit með starfseminni er hjá Póst- og fjarskiptastofnun er eðlilegt að kvörtunum vegna hennar sé beint til þeirrar stofnunar.

Í ljósi þessa verður að telja að staðsetning bannskrárákvæðisins í lögum um persónvuernd og meðferð persónuupplýsinga sé óheppileg og betra sé að staðsetja það í lögum um Þjóðskránna sjálfa og að í öðrum sérlögum verði síðan vísað til þeirrar bannskrár. Annar kostur yrði að skipta ákvæðinu upp og fella það inn í viðkomandi sérlög þ.e. fjarskiptalög og póstlög.

Þar sem Hagstofan, nú Þjóðskrá, heldur utan um almannaskráningu þ.m.t. nafn, kennitölur, heimilisföng og bannskrá vegna markpósts og það bann er fortakslaust og óháð tækni þykir eðlilegt að fjarskiptafyrirtæki samkeyri símaskrá sína við Þjóðskrá. Með því afla þau upplýsinga um þá einstaklinga sem óskað hafa eftir því að fá frið fyrir markaðssetningu í gegnum síma og geta bannmerkt númer þeirra í símaskrár. Þannig fæst samræmi milli þessara skráa sem leiðir til einföldunar og aukinnar verndar fyrir einstaklinga. Ekki er þó ætlunin með breytingunni að meina fjarskiptafyrirtækjum sem og öðrum lögaðilum að annast þjónustu varðandi bannmerkt símanúmer.[44]

Lagt er til að í 45. gr. fjarskiptalaga verði kveðið á um að virða beri bannskrá Þjóðskrár og mælt fyrir um skyldu fjarskiptafyrirtækja til samkeyrslu við skrána. Að sama skapi verði kveðið á um það í 33. gr. póstlaga nr. 19/2002 að virða beri bannskrá Þjóðskrár. Einnig verði bætt við greinina ákvæði sem heimili almenningi að hafna mark- og auglýsingapósti, sem borin er í hús, með merkingu á póstkassa og bréfalúgu. Með framangreindum breytingum má fella út sambærileg ákvæði í 28. persónuverndarlaganna.

Í gildandi lögum takmarkast ákvæðið 5. mgr. 46. gr. við notendur almennrar talsímaþjónustu, en samkvæmt skilgreiningu í 2. tölulið 3. gr. fjarskiptalaga nær það hugtak ekki til farsímaþjónustu. Hins vegar er eðlilegt að ákvæðið taki einnig til farsímanotenda.

Auk þess er lagt til að 14. gr. laga um húsgöngu og fjarsölu verði felld brott eða verði breytt þannig að hún hafi ekki að geyma sjálfstæða efnisreglu heldur vísi eingöngu til ákvæða fjarskiptalaga og póstlaga.

[44] Nú liggja fyrir tillögur til breytinga á fjarskiptatilskipunum Evrópusambandsins þar sem framkvæmdastjórnin íhugar að gera að fella símaskrá og símaskrárþjónusta út úr alþjónustu.

Í hnotskurn fela breytingarnar í sér eftirfarandi:

1. Að bannskrárákvæði 28. gr. persónuverndarlaga verði flutt í lög um Þjóðskrána sjálfa eða því skipt upp og komið fyrir í fjarskiptalögum og póstlögum. Gerðar verði aðrar breytingar á þessum lagabálkum til samræmis.

2. Breytingar á fjarskiptalögum:
a. Breytt verði 45. gr. fjarskiptalaga á þá leið að fjarskiptafyrirtækjum verði gert skylt að samkeyra símaskrár sínar við bannskrá Þjóðskrár.
b. Breytt verði orðalagi 5. mgr. 46. gr. laganna á þann veg að notendur almennrar tal- og farsímaþjónustu sem lið í markaðssetningu skuli virða bannskrá Þjóðskrár og bannmerkingar í símaskrám. Jafnframt verði kveðið á um rétt viðtakanda til að fá vitneskju um hvaðan þær upplýsingar koma sem liggja úthringingu til grundvallar.
c. Að kveðið verði á um það með skýrum hætti að 1. mgr. 46 gr. fjarskiptalaga taki einnig til smáskilaboða (SMS). Jafnframt verði 5. mgr. greinarinnar breytt í þá veru að hún taki ótvírætt til notkunar á farsíma við beina markaðssetningu þegar markpóstur er sendur með smáskilaboðum.

3. Breytingar á 33. gr. póstlaga:
a. Markaðsaðilum sem hyggjast dreifa markpósti verði gert skylt að virða bannskrá Þjóðskrár.
b. Skylt er að nafn sendanda komi fram á áberandi stað á útsendum markpósti og hvert þeir sem andmæla því að fá slíkan markpóst geti snúið sér. Viðtakandi markpósts á rétt á að fá vitneskju um hvaðan þær upplýsingar koma sem liggja útsendingu til grundvallar.
c. Dreifingaraðilum pósts ber að virða merkingar á póstkassa og bréfalúgu þar sem viðtöku markpósts og annars auglýsingarefnis er hafnað. .

4. Fella þarf brott ákvæði 14. gr. laga um húsgöngu og fjarsölu eða breyta því á þá leið að þar verði aðeins að finna almenna tilvísun til ákvæða fjarskiptalaga og póstlaga varðandi beina markaðssetningu.

Gagnlegar vefsíður á Norðurlöndum um net- og upplýsingaöryggi

Ísland
Hér er slóðin á heimasíðu Póst- og fjarskiptastofnunar
http://www.pfs.is/
Slóð á upplýsingar um net- og upplýsingaöryggi
http://www.pfs.is/displayer.asp?cat_id=25

Finnland
Slóð á heimasíðu finnsku Póst- og fjarskiptastofnunarinnar.
http://www.ficora.fi/ og á sænsku http://www.ficora.fi/ruotsi/index.html
Slóð á upplýsingar um net- og upplýsingaöryggi
http://www.ficora.fi/ruotsi/tietoturva/saadokset.htm
Einnig er að vinna slóð inn á tillögu um aðlögun á regluverkinu hér
http://www.ficora.fi/ruotsi/document/SMS11ru.pdf

Svíþjóð
Slóðin á heimasíðu sænsku Póst- og fjarskiptastofnunarinnar.
http://www.pts.se
Hér er öryggissíðan og ,,hve örugg er tölvan þín" http://www.pts.se/internetsakerhet/Sidor/startsida.asp
Slóð inn á uppl. um net- og uppl.öryggi.
http://www.pts.se/internetsakerhet/Sidor/sida.asp?Sectionid=1810

Danmörk
Slóð á heimasíðu dönsku Póst- og fjarskiptastofnunarinnar.
http://www.itst.dk/
Slóð inn á uppl. um net- og uppl.öryggi
http://www.itst.dk/wimpdoc.asp?page=tema&objno=98081575

Noregur
Slóðin á heimasíðu norsku Póst- og fjarskiptastofnunarinnar.
http://www.npt.no/
Slóð inn á uppl. um net- og uppl.öryggi
http://www.npt.no/portal/page?_pageid=121,47171,121_47182&_dad=web&_schema=PORTAL