TÖLVUMÁL

Tímarit Skýrslutæknifélags Íslands | 1. tbl. | 35. árgangur | nóvember 2010

ský

Meðal efnis:

Öryggi upplýsinga

Skýrslutæknifélag Íslands er félag einstaklinga, fyrirtækja og stofnana á sviði upplýsingatækni. Markmið félagsins eru m.a. að breiða út þekkingu á upplýsingatækni og stuðla að skynsamlegri notkun hennar og að skapa vettvang fyrir faglega umræðu og tengsl milli félagsmanna. Starfsemin er aðallega fólgin í, auk útgáfu tímarits, að halda fundi og ráðstefnur með fyrirlestrum og umræðum um sérhæfð efni og nýjungar í upplýsingatækni.

Félagsaðild er þrenns konar; aðild gegnum fyrirtæki, einstaklingsaðild og námsmannaaðild. Greitt er fullt félagsgjald fyrir fyrsta mann frá fyrirtæki, hálft fyrir annan og fjórðungsgjald fyrir hvern félaga umfram tvo frá sama fyrirtæki. Einstaklingar greiða fjórðungsgjald. Félagsgjöld 2010: Fullt gjald: kr. 21.500, hálft gjald: kr. 10.700 og fjórðungsgjald: kr. 5.400. Aðild er öllum heimil.

Þorvarður Kári Ólafsson

// Ritstjórapistill

Ágæti lesandi

Áhættumat virðist ekki hafa verið tekið mjög alvarlega í viðskiptalífinu árið 2007. Á þeim tíma hikuðu menn ekki við að taka gífulega áhættu, helst á kostnað annarra, og stjórnvöld voru ekki með neyðaráætlun sem virkaði. Afleiðingarnar þekkjum við öll. Þeir sem vilja tryggja öryggi upplýsinga þurfa hins vegar að leggja mat á þau áföll sem upplýsingarnar gætu orðið fyrir og taka meðvitaða og skjalfesta ákvörðun um þá áhættu sem þeir eru sáttir við að taka gagnvart slíkum áföllum.

Efni Tölvumála snýst að þessu sinni einkum um öryggi upplýsinga. Hér má lesa um það helsta sem hafa þarf í huga þegar unnið er með upplýsingar sem verja þarf áföllum. Lesa má góð ráð frá sérfræðingum og reynslu þeirra sem hafa komið á stjórnkerfi fyrir upplýsingaöryggi. Fjallað er um tölvuþrjóta og aðrar hættur sem steðja að upplýsingum, hvaða afleiðingar það getur haft þegar brestir verða, leiðir til varnar og mikilvægi þess að vita hvenær öryggið skiptir máli.

Að auki er í blaðinu efni af ýmsum öðrum toga, og ber þar sérstaklega að nefna að við minnumst tveggja heiðursfélaga sem nýlega féllu frá. Báðir hafa þeir sett mark sitt á störf félagsins, og svo vill til að þegar Tölvumál komu fyrst út árið 1976 var Óttar ritstjóri og Oddur varaformaður félagsins.

Ritstjórn vonast til að lesendur njóti lestursins og öðlist betri skilning á því hvenær þurfi að huga að upplýsingaöryggi og hvaða leiðir séu færar í þeim efnum.

Þorvarður Kári Ólafsson
Ritstjóri

Tölvumál er vettvangur umræðna og skoðanaskipta um upplýsingatækni sem og fyrir málefni félagsins. Óheimilt er að afrita á nokkurn hátt efni blaðsins að hluta eða í heild nema með leyfi viðkomandi greinahöfunda og ritstjórnar. Blaðið er gefið út í 1.200 eintökum.

Prentvinnsla
Litlaprent

Ritstjóri og ábyrgðarmaður:
Þorvarður Kári Ólafsson

Aðrir í ritstjórn:
Ásrún Matthíasdóttir
Ágúst Valgeirsson
Brynjar Smári Bjarnason
Helga Jóhanna Oddsdóttir

Aðsetur:
Engjateig 9
105 Reykjavík
Sími: 553 2460

Netfang:
sky@sky.is

Heimasíða:
http://www.sky.is

Framkvæmdastjóri Ský:
Arnheiður Guðmundsdóttir

Áskrift er innifalin í félagsaðild að Skýrslutæknifélagi Íslands.

TÖLVUMÁL

/ ský /

/ efni /

Ebenezer Þ. Böðvarsson,
öryggissérfræðingur CISM hjá Skýrr

Rekstaröryggi er ekki tæknivandamál heldur snýst það um manneskjur.

Starfsfólk þarf að vita hvað verið er að vernda, vera fært um að greina ákveðnar hættur og bregðast rétt við.

Öryggismeðvitund Starfsfólks

– virkjum mannlega eldvegginn

Fylgifiskur upplýsingatækninnar er að starfsumhverfið verður flóknara. Hún krefst því aukinnar þekkingar starfsfólks, meðal annars um öryggismál. Ekki er hægt að gera ráð fyrir að fólk búi yfir þessari þekkingu eða að það öðlist hana sjálfkrafa. Sú algenga trú, að tæknin dugi til að sjá fyrir vörnum, gerir illt verra. Mjög mikilvægt er að starfsfólk sé frætt um hlutverk sitt í að viðhalda mannlega eldveggnum á vinnustaðnum og að stjórnendur líti á það sem fjárfestingu að efla öryggismeðvitund starfsfólks, en ekki sem kostnað.

Hvað er öryggismeðvitund?

Öryggismeðvitund er hugtak sem notað er yfir það sem kallast á ensku „security awareness“ og verður það sífellt fyrirferðarmeira í kröfum sem gerðar eru um rekstrarumhverfi. Önnur orð yfir öryggismeðvitund eru öryggisvitund, öryggisfærni og öryggislæsi. Ýmsar skilgreiningar eru til á öryggismeðvitund en í stuttu máli má segja að starfsfólk hafi öryggismeðvitund þegar það þekkir hlutverk sitt við að tryggja rekstraröryggi vinnustaðarins, hegðar sér í samræmi við það og er fært um að taka upplýstar ákvarðanir við nýjar aðstæður. Með öðrum orðum: Það veit hvað verið er að vernda, hvers vegna og fyrir hverjum, þekkir reglur og ábyrgð og er fært um að greina ákveðnar hættur og bregðast rétt við.

Starfsumhverfi verður sífellt flóknara. Þar spila saman þættir eins og lagaumhverfi, innanhúsreglur, kröfur og fjölbreytt tækniumhverfi. Við þetta bætast stöðugt nýjar ógnir og hættur. Þetta býður upp á mistök enda er raunin sú að rekstraróhöpp verða yfirleitt af mannavöldum. Ef ekki er leitast við að stýra áhættunni ráða tilviljanir för. Stjórnendur geta ekki gert ráð fyrir ákveðinni þekkingu meðal starfsfólks nema það hafi fengið sérstaka kynningu. Þörf er á þekkingarstjórn og símenntun starfsfólks til að styrkja það í hlutverki sínu við að viðhalda mannlega eldveggnum.

Hvers vegna ætti að huga að öryggismeðvitund?

Ýmis rök mæla með því að bæta öryggismeðvitund starfsfólks. Þótt reynt sé að skýla sér á bak við fullyrðinguna um að tæknin bjargi okkur þurfa stjórnendur að átta sig á að rekstraröryggi er ekki tæknivandamál heldur snýst það um manneskjur. Skilgreina þarf öryggismeðvitund sem lykil að rekstrarsamfellu. Hún er ekki peninga- eða tímasóun heldur nauðsynleg fyrir reksturinn.

Helstu viðskiptalegu hvatir fyrir bættri öryggismeðvitund koma bæði innan úr fyrirtækjum (innri hvatir) og að utan (ytri hvatir). Til viðbótar má nefna áhættuskynjun starfsfólks. Fjölmargar innri hvatir eru til eflingar öryggismeðvitundar. Krafa um skilvirkni og aukin afköst eru góð dæmi. Niðurstöður úttekta eða áhættumats geta einnig kallað á aukna öryggismeðvitund sem og breytingar á stefnum og reglum, innleiðing nýrrar tækni eða nýleg öryggisatvik. Þá má nefna kröfu eigenda um að verja traust og ímynd fyrirtækisins. Dæmi um ytri hvatir eru til dæmis kröfur í stöðlum, svo sem ISO/IEC 27001. Samkvæmt honum skal fræða starfsmenn um öryggismál þegar þeir hefja störf, og reglulega eftir það. Ef fyrirtækið tekur á móti greiðslukortanúmerum fylgir því krafa frá kortafyrirtækjunum um reglulega fræðslu. Almennt er svo sífellt mikilvægara að starfsfólk sé upplýst um verndun persónutengdra gagna og upplýsinga.

Í sumu rekstrarumhverfi getur verið nauðsynlegt að stýra áhættuvilja og áhættuskynjun starfsfólks. Miðla þarf til þess upplýsingum um hvers vegna því beri að taka öryggi alvarlega því ekki næst hærra öryggisstig en starfsfólkið telur sjálft vera hæfilegt. Fólk er jafnan með ranghugmyndir um ógnir og áhættur sem þarf að leiðrétta.

Uppbygging áætlunar um öryggismeðvitund

Net- og upplýsingastofnun Evrópu – ENISA telur æskilegt að stýra öryggismeðvitundaráætlunum. Stofnunin leggur áherslu á að afdráttarlaus

STARFSEMI TERIS BYGGIR Á ÞJÓNUSTU, ÞEKKINGU OG ÖRYGGI

Teris er framsækið upplýsingatæknifyrirtæki, stofnað árið 1989. Viðskiptavinir Teris eru sparisjóðir, bankar, tryggingafélög, lífeyrissjóðir, opinberir aðilar og fleiri fyrirtæki.

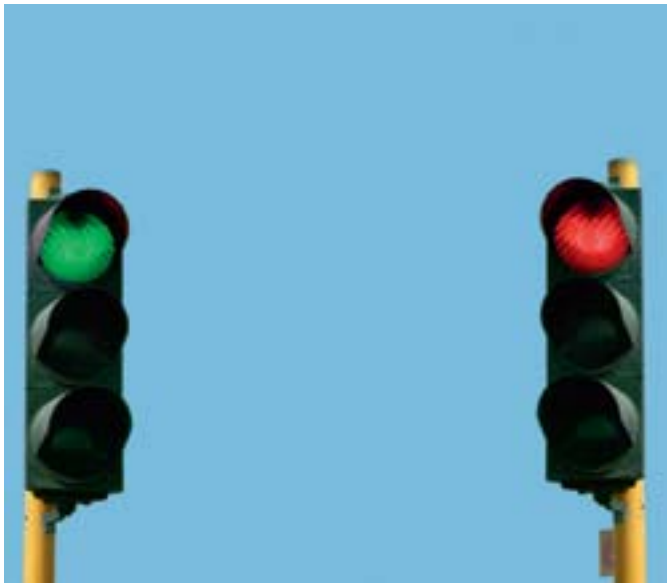
* ÖRYGGISVOTTUN TERIS STAÐFESTIR AÐ STARFSEMIN UPPFYLLIR KRÖFUR FJÁRMÁLAEFTIRLITSINS UM REKSTUR UPPLÝSINGAKERFA FYRIR EFTIRLITSSKYLDA AÐILA
* STARFSFÓLK TERIS VINNUR EFTIR SKÝRRI ÖRYGGISSTEFNU SEM SKAPAR FYRIRTÆKINU SÉRSTÖÐU Á MARKAÐI
* TILTÆKILEIKI, RÉTTLEIKI OG LEYND UPPLÝSINGA ERU HORNSTEINAR Í ÖRYGGISSTEFNU TERIS

TERIS ER VOTTAÐ SAMKVÆMT ISO/IEC 27001:2005 UM STJÓRNUN UPPLÝSINGAÖRYGGIS.

PORT hönnun

TERIS | HLÍÐASMÁRA 19 | 201 KÓPAVOGUR | SÍMI: 563 3300 | TERIS@TERIS.IS | WWW.TERIS.IS

TERIS



Aukinn trúverðugleiki næst með því að fá forstjóra til að taka þátt.

stuðningur yfirstjórnar sé forsenda fyrir því að hægt sé að auka öryggismeðvitund starfsmanna. Komi hvatinn ekki frá yfirstjórn er mikilvægt að tryggja verkefninu fullan stuðning hennar. Það er ekki aðeins forsenda þess að verkefnið fái fjármagn heldur er það lykillinn að því að árangur náist. Að auki er mikilvægt að stjórnendur gangi á undan með góðu fordæmi því ef starfsmenn fá misvísandi skilaboð er árangur ólíklegur.

Hvatarnir fyrir átakinu þurfa að liggja fyrir. Svörin við því hvað við viljum og hvers vegna verða stefnumarkandi fyrir það sem á eftir kemur. Gera þarf frávikagreiningu (gap analysis) og bera núverandi ástand saman við æskilegt ástand. Öryggismeðvitund næst með fræðslu yfir tíma (sjá mynd frá ENISA). Markmiðið næst með viðhorfsbreytingu sem leiðir til breytingar á hegðun. Til að lágmarka kostnað er gott að hafa kynningar vegna vitundarvakningar eins stuttar og hægt er, en samt nógu ítarlegar til að efnið komist til skila. Niðurstöður úr frávikagreiningu nýtast við að gera efnið hnitmiðaðra og auðvelda forgangsröðun. Sem dæmi má nefna að ef öryggisstefna fyrirtækisins eða reglur um ásættanlega notkun eigna eru ekki þekktar meðal starfsfólks þá er mikilvægt að byrja á því að kynna þær. Kynningu á atriðum sem metin eru áhættusöm út frá áhættugreiningu ætti einnig að setja í forgang sem og lærdóma sem draga má af öryggisatvikum sem upp koma til að fyrirbyggja að mistök endurtaki sig.

Mynda ætti stýrihóp sem samanstendur a.m.k. af öryggisstjóra, mannauðsstjóra, fulltrúum markaðsdeildar og framkvæmdarstjórum. Aðkoma markaðsdeildar er til þess að pakka skilaboðunum í skemmtilegar og áhugaverðar umbúðir og „selja“ öryggið.

Kostnað þarf að ákveða í upphafi en hann þarf ekki endilega að vera mikill. Hvernig verður skilaboðunum til starfsfólks miðlað? Á að nota innri vef, kennslukerfi, fyrirlestra, sýnikennslu, fundi, myndbönd, plaköt, fréttabréf, próf, fréttaúrklippur og fá aðstoð frá sérfræðingum? Dæmi um ódýra miðlun er að hafa reglulega 20 mínútna fyrirlestra yfir hádegisverði. Sum atriði eiga við alla starfsmenn en önnur ekki. Markhópar sem gætu þurft sérsniðin námskeið eru t.d. kerfisstjórar, stjórnendur, fjarnotendur, hugbúnaðargerðar-, framlínu- og sölufólk. Skynsamlegt er að gera langtímaáætlun til að tryggja að verkefninu sé sinnt vel og að það koðni ekki niður í hversdagslegu annríki.

Upphafið skiptir höfuðmáli fyrir það sem á eftir kemur. Það á jafnt við um við hvernig öryggisstefnan er kynnt við móttöku nýrra starfsmanna og þegar gert er átak innan fyrirtækisins í tengslum við afmörkuð öryggismál. Aukinn trúverðugleiki næst með því að fá forstjóra til að taka þátt í og kynna hvert átak. Það undirstrikar hversu mikið er lagt upp úr öryggi innan fyrirtækisins.

Mælingar eru mikilvægar

Mælingar eru mikilvægar bæði vegna áætlunar um fjármögnun næsta árs og til að svara spurningunni: „Hefur okkur eitthvað miðað áfram frá því í fyrra?“ Menn eru ekki á einu máli um hvaða mælikvarðar eru hentugastir en samkvæmt könnun ENISA nota flestir mælingar úr innri og ytri úttektum. Við það má bæta að ef vandað er til verka getur könnun meðal starfsmanna gefið gagnlega innsýn inn í þætti sem stuðla að öruggri hegðun, svo sem spurningar um hvert fordæmi stjórnenda sé, hvað þekkingu viðkomandi hafi, hvaða viðhorf hann hafi til öryggismála og hvað fái hann til að sinna þeim. Beita má margvíslegum aðferðum við mælingar. Almennt er æskilegt að þær séu: hlutlægar og endurtakanlegar, ódýrar í framkvæmd, niðurstöður séu settar fram sem tölustafur með mælieiningu og að þær hafi merkingu þannig að hægt sé að bregðast við.

Sú hætta er alltaf fyrir hendi að dregnar séu rangar ályktanir af mælingum. Fjölgun skráðra öryggisatvika er til dæmis, þvert á það sem mörgum kann að finnast, merki um aukna öryggismeðvitund. Hún sýnir að fólk þekkir bæði öryggisatvik og veit hvernig á að tilkynna þau. Varast ber að koma upp hvatakerfum sem miða að því að fækka skráningu öryggisatvika því þau gefa ranga mynd af ástandinu. Þó skal bent á að umbun er yfirleitt betri leið en refsing til að breyta hegðun fólks.

Fyrsta dauðsfall áhættuleikarans

Öryggismeðvitund verður ekki til með einum fyrirlestri og ekki er til pakkalausn sem hentar öllum fyrirtækjum. Mörgu má sinna með innanhússþekkingu og -kröftum en öðru með aðstoð aðkeyptra sérfræðinga. Hvort sem áhugi er fyrir því að breyta öryggismenningu fyrirtækisins eða plástra helstu þekktu veikleikana er mikilvægt að byrja rétt og nýta reynslu annarra.

Vandinn er og verður til staðar en það þarf að takast á við hann og hætta að benda á „heimsku notendurna sem hlusta ekki á neitt“. Úrtöluröddum sem segja að aukin öryggismeðvitund sé óþarfi því ekkert hafi komið fyrir hingað til má svara með því að benda á að fyrsta dauðsfall áhættuleikarans er jafnframt hans síðasta.

Heimildir

ENISA (2007). Information security awareness initiatives: Current practice and the measurement of success. Sótt 15. apríl, 2010 frá ENISA: http://www.enisa.europa.eu/act/ar/deliverables/2007/kpi-study/en

ENISA (2008). The new users' guide: How to raise information security awareness. Sótt 15. apríl, 2010 frá ENISA: http://www.enisa.europa.eu/act/ar/deliverables/2008/new-users-guide

ENISA (2009). Information security awareness in financial organisations - Guidelines and case studies. Sótt 15. apríl, 2010 frá ENISA: http://www.enisa.europa.eu/act/ar/deliverables/2009/is-in-financial-organisations-09

Jaquith, A, (2007). Security Metrics: Replacing Fear, Uncertainity, and Doubt. Pearson Education, Inc.

NIST (2003). SP 800-50 Building an Information Technology Security Awareness and Training Program. Sótt 15. apríl, 2010 frá http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Bjargey Guðmundsdóttir, gæða- og öryggisstjóri Þjóðskrá Íslands (áður Fasteignaskrá Íslands)

Ef samfélagið bæri ekki traust til upplýsinganna væri stofnunin ekki mikils virði.

Hvers virði er upplýsingaöryggi fyrir grunnskrár ríkisins?

Þann 1. júlí sl. tóku gildi lög um sameiningu Þjóðskrár og Fasteignaskrár Íslands undir nafninu Þjóðskrá Íslands. Eftirfarandi grein var skrifuð fyrir sameininguna og fjallar um vottað stjórnkerfi upplýsingaöryggis hjá Fasteignaskrá, en síðan þá hefur verið unnið að því að vottunin nái til allrar starfsemi Þjóðskrár Íslands.

Innleiðing staðalsins

Fasteignaskrá Íslands varð árið 2006 fyrst íslenskra stofnana til þess að fá starfsemi sína vottaða samkvæmt ISO 27001 staðlinum um öryggi upplýsinga en vinna við innleiðinguna og undirbúningur fyrir vottun hófst árið 2004. En hvers vegna var ákveðið að innleiða þennan staðal hjá Fasteignaskrá? Ef samfélagið bæri ekki traust til starfsemi Fasteignaskrár og þeirra upplýsinga sem hún geymir væri stofnunin ekki mikils virði. Verkefni stofnunarinnar eru líka þess eðlis að upplýsingaöryggið skiptir miklu máli, samstarfsaðilar Fasteignaskrár byggja mikilvæga þætti í sinni starfsemi á þessum upplýsingum.

Fasteignaskrá Íslands tók til starfa árið 1977 en hét þá Fasteignamat ríkisins, og heyrir stofnunin undir dómsmála- og mannréttindaráðuneytið. Stjórn Fasteignaskrár er skipuð fulltrúa frá ráðuneytinu, einum fulltrúa frá sveitarfélögunum og einum frá tryggingafélögunum. Helstu verkefni Fasteignaskrár eru að hafa yfirstjórn fasteignaskráningar og sjá um rekstur fasteignaskrár, meta fasteignir fasteignamati og brunabótamati, skrá þinglýsta kaupsamninga og vinna úr þeim upplýsingar um fasteignamarkaðinn ásamt því að gefa árlega út fasteignaskrá. Af þessu sést að það eru víðtækar upplýsingar sem eru geymdar hjá Fasteignaskrá um byggingar, land og fasteignamarkaðinn. Þessum upplýsingum er síðan miðlað á heimasíðu stofnunarinnar skra.is bæði til almennings og til þeirra sem nota upplýsingarnar í sínu starfi. Fjölmörg fyrirtæki og stofnanir fá einnig aðgang að skránni í gegnum vefþjónustur.

Skráningaraðilar og upplýsingar í fasteignaskrá

Á heimasíðunni er hægt að fletta upp fasteignum með því að slá inn heimilisföng. Upplýsingarnar sem þá birtast eru helstu stærðir mannvirkja og skipting þeirra í minni fasteignir, notkun mannvirkja og lands, byggingarefni og byggingaár ásamt staðsetning á loftmynd. Einnig er hægt að fá áskrift að nánari upplýsingum um fasteignir og eigendur þeirra ásamt veðbandayfirliti úr þinglýsingahluta fasteignaskrár.

En það eru margir aðilar sem skrá upplýsingarnar. Tilgangurinn með skránni er ein skrá fyrir mörg stjórnvöld og er helsta markmiðið að koma í veg fyrir tvískráningar og misræmi milli ólíkra skráningaraðila. Allar upplýsingar í fasteignaskrá nema matsupplýsingar koma frá öðrum stjórnvöldum. Byggingafulltrúar sveitarfélaganna skrá stærðir og eignaskiptingu, starfsmenn sýslumanna skrá eigendur og veðbönd og tryggingafélög skrá brunatryggingar svo eitthvað sé nefnt. En það er hlutverk Fasteignaskrár að fara með yfirumsjón með skráningunni hjá öllum þeim aðilum sem skrá upplýsingarnar.

Þeir aðilar sem nota síðan upplýsingarnar úr skránni eru fjölmargir. Helst mætti nefna sveitarfélögin sem nota skrána og fasteignamatið sem grundvöll fyrir álagningu fasteignagjalda en þetta er gert í sérstöku álagningakerfi sem Fasteignaskrá rekur fyrir sveitarfélögin. Tryggingafélögin nota fasteignaskrá til þess að halda utanum tryggingar og reikna út iðgjöld vegna brunatrygginga. Og fasteignasalar eru farnir að miða við fasteignamat í auknum mæli þegar þeir verðmeta fasteignir en þeir nota líka uppýsingar um skráðar stærðir í fasteignaskrá ásamt veðbandayfirlitum úr þinglýsingahluta. Íbúðalánasjóður og aðrar fjármálastofnanir eru einnig stórir notendur vegna lána með veðum í fasteignum. Allar þessar upplýsingar eru á rafrænu formi en að auki geymir Fasteignaskrá eitt stærsta safn mannvirkjateikninga á öllu landinu.

Aðgangsstýring

Af öllu þessu má sjá hvaða þýðingu upplýsingaöryggi hefur í starfseminni. En það er ekki nóg að halda upplýsingunum leyndum fyrir þeim sem ekki eiga að fá aðgang að þeim, það þarf líka að tryggja aðgengi að þeim fyrir þá sem á þeim þurfa að halda í sínu starfi. Aðgangsstýring í tölvukerfin er því mikilvægur þáttur í starfseminni. Starfsmenn Fasteignaskrár Íslands eru nú rúmlega 50 talsins á þremur skrifstofum, í Reykjavík, á Selfossi og á Akureyri. Virkir aðgangar í kerfi Fasteignaskrár eru 73 hjá byggingafulltrúum sveitafélaganna, 534 hjá starfsmönnum sem starfa við álagningu fasteignagjalda hjá sveitarfélögum og 253 sem starfa á skrifstofum sýslumannsembætta.

Aðilar sem hafa starfs síns vegna fengið aðgang í fasteiganaskrá og veðbandayfirlit eru nú 618 talsins. Þetta eru td. fasteignasalar, lögmenn, fjármálastofnanir og tryggingafélög. Árið 2008 voru samtals 22 virkar vefþjónustur og voru 40 þúsund skeyti seld til þeirra. Í júní 2009 voru þær 19 og seld skeyti um 23 þúsund. Fjórar vefþjónustur eru til heildsala sem síðan selja þjónustuna áfram til sinna viðskiptavina.

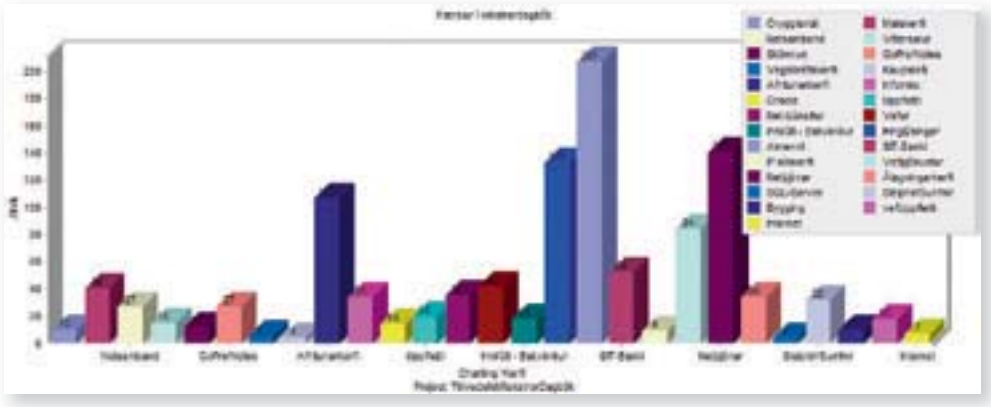
Upplýsingaöryggi í framkvæmd

Upplýsingaöryggi er einnig mikilvægur þáttur í rekstri tölvukerfa hjá Fasteignaskrá. Öll upplýsingaverðmæti þarf að skrá og þau þurfa að hafa ábyrgðarmenn. Þar er ekki bara tölvubúnaður og hugbúnaður sem er talin til verðmæta, þekking starfsmanna og verkferlar eu líka skráðir ásamt trausti og ímynd stofnanarinnar svo eitthvað sé nefnt. Breytingastjórnun þarf að vera á öllum kerfum og skjölum vegna öryggiskerfisins. Innri úttektir fara fram fjórum sinnum á ári og ytri úttekt er einu sinni á ári.

Rekstrardagbækur þarf að rýna með reglulegu millibili en í þær eru skráð öll rekstraratvik og þau flokkuð. Aðgerðir til úrbóta eru síðan framkvæmdar samkvæmt niðurstöðum.

Öll upplýsingaverðmæti þarf að skrá og þau þurfa að hafa ábyrgðarmenn.

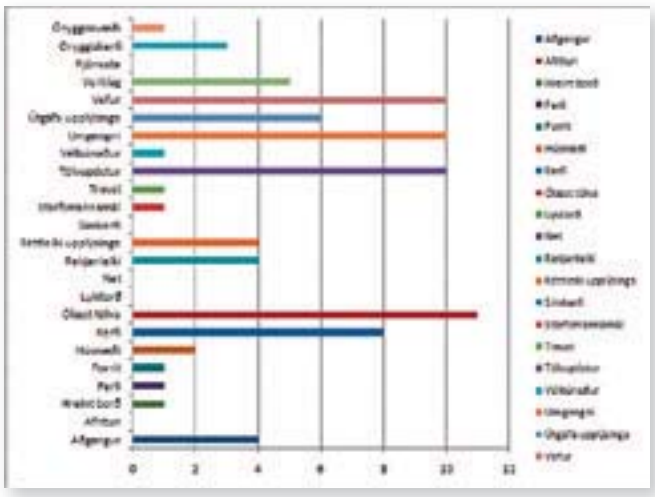
Starfsmenn bera allir sameiginlega ábyrgð á að tilkynna um öll öryggisatvik sem upp koma.



Dæmi um flokkun skráningar í rekstrardagbók Fasteignaskrár Íslands.

Áhættumat fer fram einu sinni á ári á öllum skráðum verðmætum í verðmætaskrá. Einnig er gert áhættumat ef sérstaklega er þörf á. Sem dæmi um tilvik má nefna að við hrun bankanna haustið 2008 var framkvæmt áhættumat vegna hættu á gjaldeyrisskorti og þeim áhrifum sem það gæti haft á rekstur tölvukerfanna hjá Fasteignaskrá og þegar nafni stofnunarinnar var breytt úr Fasteignamat ríkisins í Fasteignaskrá Íslands 1. janúar 2008. Þá þurfti að fara fram kynningastarf með samstarfsaðilum og breyta vef stofnunarinnar og útliti vefsins. Samkvæmt staðlinum er áhættumat alltaf framkvæmt þegar breytingar eiga sér stað í starfseminni og í tölvukerfunum. Aðrir mikilvægir þættir í upplýsingaöryggginu er neyðaráætlun en hún þarf að vera til staðar ef starfsemin stöðvast af einhverjum orsökum td náttúruhamförum eða bruna. Þá er ekki síður mikilvægt að daglegar afritanir séu teknar af öllum gögnum í skránni.

Upplýsingaöryggi á við vinnu allra sem vinna hjá Fasteignaskrá. Allir nýir starfsmenn fá fræðslu um öryggismál á fyrstu vikum í starfi en þau eru líka rifjuð upp árlega með öllum starfsmönnum. Starfsmenn bera allir sameiginlega ábyrgð á að tilkynna um öll öryggisatvik sem upp koma. Það er gert með því að senda tölvupóst á sérstakt netfang en gæða- og öryggisstjóri hefur það hluverk að vinna úr tilkynningunum og sjá til þess að aðgerðum vegna þeirra sé fylgt eftir.



Flokkun öryggistilkynninga ársins 2009

Oft er erfitt að greina á milli þess hvort tilkynnt atvik er öryggismál eða gæðamál en tekin var sú ákvörðun að reyna ekki að flokka tilkynningarnar heldur að taka við öllum ábendingum sem berast frá starfsmönnum og afgreiða þær. Þannig tækist best að virkja alla starfsmenn og öryggisvitund þeirra.

Verkefnin framundan

En til hvers að standa í þessu öllu saman? Er þetta allt saman fyrirhafnarinnar virði því vissulega virðist þetta tímafrekt fyrir hinn almenna starfsmann? Fasteignir eru stærsta eignasafn landsmanna. Ævisparnaður fólks á Íslandi fer oftast í fasteignir og þær eru oft hluti af lífeyri fólks á efri árum. En fasteignir eru líka notaðar sem trygging fyrir veði í lánaviðskiptum og atvinnulífið fær þaðan fjármagn til reksturs. Og eins og sagði hér í upphafi þá byggja fjölmargar aðrar stofnanir lögbundna starfsemi sína á upplýsingum úr fasteignaskrá. Til þess að þær geti sinnt sínum störfum verða þær að geta treyst á að upplýsingarnar sem unnið er með séu réttar og aðgengilegar þegar á þarf að halda.

Nú þegar ríkið er að draga saman seglin eru uppi margar hugmyndir um sameiningu stofnana. Ein hugmyndin sem komið hefur fram af hálfu ríkisstjórnarinnar er að stofnuð verði sérstök grunnskrá ríkisins þar sem td fasteignaskrá, þjóðskrá, ökutækjaskrá og jafnvel fleiri skrár verða sameinaðar. Auknir möguleikar verða í miðlun og samþættingu upplýsinga við sameiningu þessara skráa. Alþingi hefur þegar samþykkt lög um sameiningu Fasteignaskrár og Þjóðskrár. Áherslan hjá stjórnvöldum hefur í auknum mæli verið að efla rafræna stjórnsýslu en þar er talið að hægt sé að spara umtalsverðar fjárhæðir fyrir samfélagið. Einn liður í því er að koma á rafrænum þinglýsingum og verður Fasteignaskrá ein þeirra stofnana sem taka þátt í því verkefni.

Það er ljóst að vottun í öryggi upplýsinga hefur gefið Fasteignaskrá ákveðna sérstöðu í aðkomu að nýjum verkefnum, vottunin hefur aukið traust stjórnvalda á því að stofnunin sé í stakk búin að taka að sér flókin verkefni í samvinnu við aðrar stofnanir, sveitarfélög og atvinnulífið. En ávinningurinn fyrir samfélagið er líklega enn meiri. Upplýsingarnar verða áreiðanlegri og aðgangur allra er tryggður. Þannig myndast meira jafnræði milli þeirra sem upplýsingarnar varða.

Ertu með Sjónvarp Símans?

Þú leigir þér mynd eða þátt með einum takka á fjarstýringunni þinni. Frábær myndgæði, úrvals dagskrá og yfir 3700 titlar. Möguleiki á áskrift að yfir 60 erlendum sjónvarpsstöðvum.

Þú getur fengið þér áskrift að Sjónvarpi Símans með tvennum hætti:

- **ADSL** – hægt að fá 2 myndlykla
  Hámarkshraði á interneti er 16 Mb/s
- **LJÓSNET** – hægt að fá 5 myndlykla
  Hámarkshraði á interneti er 50 Mb/s

800 7000 – siminn.is

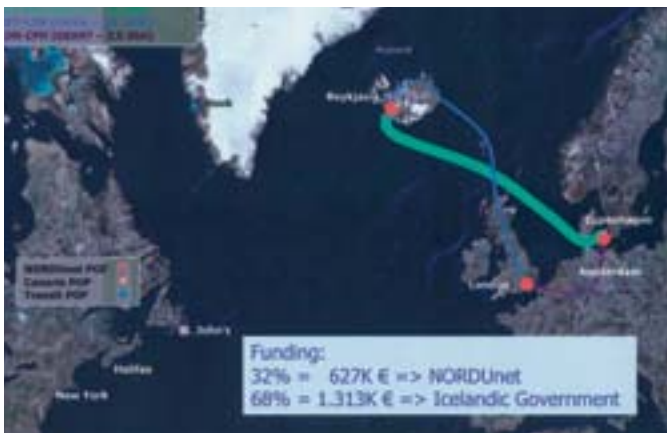
Það er **Síminn**

Sæþór L. Jónsson MScEE, varaformaður stjórnar NORDUnet A/S

Íslensk stjórnvöld bera engan kostnað af verkefninu.

NORDUnet setur upp háhraða tengingar til Íslands

Rannsókna- og háskólanet Íslands (RHnet) hefur frá miðju ári 2003 unnið að því að bæta utanlandstenginguna til NORDUnet, sem sér rannsókna- og háskólanetum Norðurlanda fyrir tengingun við öll sambærileg net í heiminum. Upphaflega var ætlunin að íslensk stjórnvöld kæmu að málinu með samningum menntamála- samgöngu- og forsætisráðuneytanna við Farice hf, sem er eigandi sæstrengja sem tengja Ísland. Áætlaður kostnaður var um 1,9 MEUR. Greiðsluskiptingin yrði þannig að 68% af greiddist af íslenskum stjórnvöldum, þ.e. um 1,3 MEUR og 32% af NORDUnet eða um 0,6 MEUR. Þetta gekk ekki eftir, en sýnir hve kostnaðarsamar tengingar hjá Farice voru og eru í raun enn, þótt þær hafi lækkað nokkuð nýverið.



Mynd 1. Síðasta áætlun (2007) um tengingu RHnet við NORDUnet með þátttöku yfirvalda

Góðir samningar

Sumarið 2009 tókst NORDUnet að semja við Farice og eigendur grænlenska strengsins „Greenland Connect“ og ná þannig tengingu milli Danmerkur, Íslands og Ameríku. Frá lendingarstað Greenland Connect í Ameríku var samið við kanadíska rannsókna og menntanetið, Canarie, um tengingu til þeirra og jafnframt að þeir myndu útvega tengingu áfram til New York. Einn vendipunktur í þessu ferli var einnig styrkur frá National Science Foundation (NSF) í Bandaríkjunum til að styrkja tengingar um norðurhjarann milli Evrópu og Bandaríkjanna. Ákveðið var að tengja NORDUnet við Internet2 í New York og skiptast á rannsóknaumferð þar með viðkomu á Íslandi. Með því yrði Ísland tengiliður evrópsku og bandarísku rannsóknanetanna. Netkerfi Internet2 er með því öflugasta sem gerist í heiminum í dag og tengist öllum helstu háskólum og rannsóknastofnunum Bandaríkjanna. Sambærilegt net í Evrópu er Géant3 sem NORDUnet er jafnan talinn hluti af.

Kostnaðurinn við að koma þessum tengingum á er að mestu borinn af NORDUnet og er ríflega sú upphæð sem þeir hafa sett í tengingu RHnets frá 2001, en þeir hafa til þessa keypt sambönd í gegnum CANTAT-3 af Tata Communications. Framlag NORDUnet er um 85,5% af heildarkostnaði og mótframlag NSF í USA er um 14,5%. Íslensk stjórnvöld bera engan kostnað af verkefninu. NORDUnet hefur því náð að spara yfirvöldum umtalsverða fjármuni frá fyrri áætlun (vel á aðra milljón evra á ári) og koma jafnframt með fjármuni inn í íslenska hagkerfið með kaupum á þessum samböndum. Núverandi (júní 2010) tengingar RHnet eru:

- 10 Gbs á Danice til Kaupmannahafnar
- 2,5 Gbs á Farice til London

Þessar nýju tengingar gjörbylta landslaginu fyrir hið íslenska rannsókna og háskólasamfélag.

Með þessari uppbyggingu er minnkuð sú gjá sem Norðurhjarasvæðin hafa búið við.

Mjög fljótlega er svo reiknað með að taka í notkun 4 Gb/s samband á Greenland Connect og þá yrðu tengingarnar í fyrstu svo:

- 2 Gbs til Canarie í Halifax
- 2 Gbs áfram til New York.

Innan tveggja til þriggja ára er svo reiknað með að ekkert þessara sambanda verði minna en 10 Gb/s.

Mynd 2. Tengingar RHnet í júní 2010

Mynd 3. Fyrirhugaðar tengingar NORDUnet 2012

Það er von okkar að á næstu árum verði lagður nýr sæstrengur milli Íslands og Ameríku, þannig að um Ísland geti farið drjúgur hluti umferðarinnar milli heimsálfanna. Mikill áhugi er fyrir þessum tengingum í Evrópu, Bandaríkjunum, Kanada og víðar. Þyrftu yfirvöld að hafa þarfir vísindasamfélagsins í huga og veita aðgang að pari í fyrirhuguðum strengjum, svo fremi sem yfirvöld koma að kostnaði við lagningu þeirra.

Samningurinn við NFS er til tveggja ára, en er framlengjanlegur. NORDUnet hefur gert þriggja ára áætlun fyrir þetta verkefni og stefnir á 10Gbs hring innan þess tíma. Styrkurinn frá NSF tengist viðbót þeirra við uppbygginu (frá 1997) á samtengineti fyrir rannsakendur um allan heim sem nefnt er Global Ring Network for Advanced Applications Development (GLORIAD) og með núverandi aukningu (sem er einn hringur í viðbót um heiminn) kallað GLORIAD-Taj. Í þessari uppfærslu bætast m.a. við sérstakir tengipunktar í Alexandríu í Egyptalandi, Indlandi, Hong Kong, Singapore, Mumbai, Amsterdam og Kaupmannahöfn. (Er gert með samstarfi við Tata Communications, en framlag þeirra er metið á um sex milljónir dollara.)

Opnar nýja möguleika

Þessar nýju tengingar gjörbylta landslaginu fyrir hið íslenska rannsókna og háskólasamfélag, en álag á þau tiltölulega rýru sambönd sem RHnet hafði áður til útlanda var orðið mikið.

En hvaða tækifæri opna þessar tengingar? Þar má nefna :

- Hýsing stórra gagnavera sem byggja á endurnýjanlegri „grænni“ orku
- Ofurtölvumiðstöð Norðurlanda, Nordic HPC (High Performance Computing)
- Þáttaka í rannsóknaverkefnum í Evrópu, USA og víðar
- Rannsóknum á sviði jarðfræði, jarðhita, stjörnufræði og líftækni
- Samstarf við Kínverja og Indverja

Eins og áður kom fram er NORDUnet er með tengingar við Evrópunetið Geant3 og Internet2 í USA. Þessi tvö net eru öflugustu samtenginet veraldar og eru jafnframt með öflugar tengingar um allan heim.

Í gegnum samvinnu NORDUnet um „IceLink“ hugmynd sína og NSF um uppbyggingu þeirra á GLORIAD-Taj, tengist Norðurpóls svæðið með 10 Gbs. Það tengir þannig USA við Grænland, Norðurlöndin og Rússland. Rannsakendur á áhrifum hlýnunar jarðar og áhrifanna á Norðurpólssvæðið geta flutt gögn með nýjustu nettækni til heimahaga. Samruni Gloriad-Taj og Icelink verkefnanna er skínandi dæmi um samstarf rannsóknasjóða og rannsókna- og mennntaneta um allan heim. Með þessari uppbyggingu er minnkuð sú gjá sem Norðurhjarasvæðin hafa búið við varðandi öflugar tengingar. Góðar og öruggar tengingar opna jafnframt möguleika á uppbyggingu tölvuþyrpinga í tiltölulega svölu/köldu umhverfi (minni kæliþörf) og jafnframt aðgang að endurnýjanlegri „grænni“ orku. Mikil reiknigeta er nauðsynleg fyrir ýmsa vísindalega útreikninga og líkangerð. Fyrir vísindageirann er því ekki síður mikilvægt að hjálpartæki þeirra séu knúin á endurnýjanlegri „grænni“ orku sem frekast er kostur.

Bergur Kristinsson, sérfræðingur og ráðgjafi hjá Opnum kerfum

Kerfið sem notar gögnin veit í raun ekkert hvað liggur að baki.

Tenging tækja við gagnaskýið verður einfaldari og fjölhæfari.

SNIA eru samtök framleiðenda, seljenda og notenda á sviði gagnavistunar.

Gagnaský

Í gegnum árin hafa menn byggt upp reikniafl með því að draga til sín örgjörva eftir þörfum úr „skýi“ tölva sem tengdar eru saman yfir Internetið, fyrirbærið kallast „cloud computing“ og byggir á því að þegar þörf er á miklu reikniafli er það dregið úr skýinu og að sama skapi ef ekki er þörf á öllu aflinu er því skilað til baka til annara nota.

Gagnaský er í raun ekki nýtt hugtak og hugmyndafræðin er sú sama og með reikniaflið, þ.e. að hægt sé að draga til sín gagnageymslu pláss byggt á raunverulegri þörf eða umbeðnu þjónustustigi og skila því aftur þegar ekki er þörf á því lengur. Þetta þýðir að ekki þarf að fjárfesta miðað við hugsanlega eða tímabundna þörf, heldur er einungis greitt fyrir raun notkun.

En hvernig nýtist gagnaský? Hægt er að horfa á gagnaský sem mismunandi þjónustu, hugsanlega sem aðkeypt þjónusta frá hýsingaraðila, eða sem ský innan fyrirtækis sem þjónustar margar deildir eða útibú. Ef við tökum einfalt dæmi og horfum t.d. á disk í fartölvu, notandi tölvunnar er á ferðinni um heiminn, eða innan fyrirtækisinns, þar sem hann stoppar tengist hann skýinu. Notandinn getur vistað gögnin sín í skýið. Tæknin inni í skýinu tryggir að notandinn hefur aðgengi að gagnasvæði sem getur stækkað og minnkað eftir þörfum og uppfyllir það þjónustustig sem farið er fram á við vistun gagnanna. Sama hugmyndafræði á við um netþjóna, gagnagrunna og aðrar þjónustur, byggt á óskum kerfanna um þjónustustig er gagnasvæðum úthlutað og kostnaður mældur miðað við notkun. Skýið sem slíkt byggir á mismunandi gagnakerfum, sem mynda þau þjónustustig sem boðið er upp á úr skýinu. Kerfið sem notar gögnin, hvort sem það er fartölva eða gagnagrunnsþjónn, veit í raun ekkert hvað liggur að baki, svo lengi sem umbeðið þjónustustig er uppfyllt.

Staðan

En hvar stöndum við með þessa tækni og hvenær getum við farið að nota þetta? Gagnaský eru í raun allt í kringum okkur nú þegar í sinni einföldustu mynd, þó langt sé í land ennþá. Einhverjir kannast t.d. við að greiða fjarskiptafyrirtækjunum fyrir að vista ljósmyndir eða afrita gögn, notandinn veit ekki hvar hann er að vista gögnin, þau eru bara á „Netinu“. Það eina sem notandinn veit er að hann hefur aðgengilegt pláss til að vista myndirnar sínar eða afrita gögnin sín, og þjónustuaðilinn tryggir skilgreint öryggi og aðgengi gagnanna.

En á meðan gagnaský tekur á sig mynd og þróast getur það verið erfitt að skilgreina tæknina á bakvið og hver markhópurinn er. Þó eru tveir megin þættir sem sennilega munu drífa þessa þróun áfram, en það er annars vegar óskir um gagnavistun eftir þörfum eða gagnaský í sinni eiginlegu mynd og hins vegar afritun / endurheimt gagna. Þetta eru tvær mjög líkar þjónustur en þó mismunandi. Báðar krefjast þess að hægt sé að skala gagnageymslupláss upp og niður, að utanumhald og stjórnun sé einföld, aðgengi sé sveigjanlegt og skýið geti á einfaldan hátt tengst og tekið við af núverandi kerfum.

Með auknum áhuga á gagnaskýjum hefur mikið verið rætt um eiginleika og öryggi í þannig umhverfi. En hvert stefnir þessi tækni, er þetta ennþá bóla eða er þetta í raun eitthvað sem við erum að fara að sjá og upplifa sem valkost í gagnavistun? Margir notendur og stjórnendur tölvukerfa eru þegar farnir að horfa til þeirra möguleika sem gagnaský opna, svo sem að geta meðhöndlað og fært til gögn á mismunandi miðla og staðsetningar. Fyrirheit um meiri afköst, sveigjanleika og mun ódýrari gagnavistun teljast einnig kostir sem vert er að skoða og auka þar með tiltrú manna og drífa áfram hönnun og þróun.

Núverandi efnahagsástand hefur gert mörgum fyrirtækjum erfiðara fyrir að bæta við auknu gagnarými í gagnamiðjur, en á sama tíma hefur það gagnamagn sem við búum til stóraukist og þörfin fyrir tímabundna gagnavistun er meiri. Það að hafa aðgengi að gagnavistun sem aðlagast rauntíma þörf, bæði hvað varðar stærð og kostnað, mun því verða áhugaverður kostur fyrir mörg fyrirtæki.

Hver svo sem endanleg skilgreining á gagnaskýi verður er ljóst að hugmyndafræðin leysir mörg þeirra vandamála sem stjórnendur tölvukerfa standa frammi fyrir. Fyrirtæki munu ekki þurfa að velja sér eitt ákveðið þjónustustig fyrir gagnavistun eins og oft verður þegar fjárfest er í diskakerfi, heldur verður hægt að stilla þörfina í samræmi við eðli þeirra gagna sem þarf að geyma. Kostnaður við gagnavistun verður raunhæfur, þar sem einungis er greitt fyrir notað pláss hverju sinni. Tenging tækja við gagnaskýið verður einfaldari og fjölhæfari, gagnaaðgengi sveigjanlegra og meðhöndlun gagna í samræmi við eðli þeirra og innihald.

Gagnavistunarfélagið

Þróun og skilgreining á gagnaskýi er ein af megin stefnum Storage Networking Industry Association (SNIA) og mikið fjallað um það í miðlum þeirra. SNIA eru samtök framleiðenda, seljenda og notenda á sviði gagnavistunar. Hlutverk SNIA er að samræma virkni og þróun með því að búa til og kynna staðla, tækni og menntun á sviði vistunar og meðhöndlunar gagna. Þessu er náð fram með því að mynda faglega tæknihópa með þversniði framleiðenda, seljenda og notenda gagnavistunar ásamt rástefnuhaldi og kynningum. Helstu svið SNIA eru gagnavistun í sýndarumhverfi, gagnavistun í gagnaskýi og gagnanet til tengingar gagnavistunar.

SNIA rekur upplýsingaveitu á vef sínum með upplýsingum og fræðslu. Á vegum þess eru faghópar sem annast utanumhald og framkvæmd einstakra verkefna. SNIA hefur einnig á sínum snærum fyrirlesara sem tilbúnir eru til að halda kynningar og fyrirlestra um gagnavistun óháða framleiðendum eða seljendum. Þau fyrirtæki sem aðilar eru að SNIA geta tekið þátt í og nýtt sér þessa þjónustu. En aðild að SNIA veitir meðlimum innsýn í innsta hring framtíðarsýnar og þróunar á gagnavistun og meðhöndlun gagna

SNIA hefur náð umtalsverðum árangri í viðleitni sinni til að gera gagnavistun og gagnameðhöndlun auðskiljanlegri og einfaldari í innleiðingu. Þeir staðlar sem SNIA hefur komið á hafa leitt til þess að samskipti gagnakerfa frá mismunandi framleiðendum eru auðveldari, stjórn og eftirlitskerfi samræmdari og aðgengi að gögnum skilvirkari. Meðal þeirra staðla sem SNIA hefur skilgreint á þessu sviði eru t.d. SMI-S, sem er staðall um samskipti á milli tækja á gagnaneti og stjórn eftirlitsbúnaðar og XAM, sem er staðall fyrir aðgengi að og geymslu gagna, aðallega notaður í langtímageymslu á gögnum og aðgengi að þeim eftir langan tíma.

Uppbygging og starf SNIA byggir á því að í hverju landi eða hópi landa er stjórn sem heyrir undir yfirstjórn hverrar heimsálfu, en SNIA á fulltrúa í flestum löndum heimsins. Ísland heyrir undir SNIA-Nordic sem aftur heyrir undir SNIA-Europe. Opin kerfi eiga aðild að SNIA og höfundur þessarar greinar á sæti í stjórn SNIA-Nordic. Nánari upplýsingar um SNIA má finna á vefsvæðinu www.snia.org

Steinn Jóhannsson, forstöðumaður kennslusviðs Háskólans í Reykjavík

Fyrir tveimur áratugum var hugtakið kennslukerfi óhugsandi en í dag er þetta hluti af daglegu lífi flestra stúdenta sem stunda nám á framhalds- og háskólastigi.

Hvaða persónuupplýsingar þarf að gæta sérstaks öryggis með? Hér er átt við gögn sem tengjast námsferlum, próf og úrlausnir nemenda sem eru vistuð í gagnagrunna og ýmiss konar fylgigögn á rafrænu formi sem nemendur senda með umsóknum.

Upplýsingakerfi skóla, notkun og öryggi

Í skólaumhverfi nútímans er æ meiri áhersla lögð á notkun upplýsingakerfa. Þau kerfi sem skólar nota eru jafnan nefnd „Learning Management Systems“ (LMS) á ensku en á íslensku er talað um kennslukerfi, námsumsjónarkerfi eða námsnet. Hér verður notað orðið upplýsingakerfi því verið er að ræða um umfangsmeiri kerfi en kennslukerfi. Það er ljóst að þróun í upplýsingakerfum hefur verið mjög ör síðustu árin og fullyrða má að þau kerfi sem er notast við í dag muni taka miklum breytingum á næstu árum. Fyrir tveimur áratugum var hugtakið kennslukerfi óhugsandi en í dag er þetta hluti af daglegu lífi flestra stúdenta sem stunda nám á framhalds- og háskólastigi.

Þróunin hefur verið mjög hröð síðustu ár og hefur framboð þeirra kerfa sem skólar geta valið úr aukist ár frá ári. Oft á tíðum er erfitt fyrir skóla að velja kerfi sem uppfyllir mjög svo mismunandi þarfir eftir skólastigum og markmiðum skóla. Kerfin geta verið mjög fjölbreytt og stór í sniðum og má fullyrða að skólar hafa þurft á síðustu árum að eyða æ meiri peningum í rekstur slíkra kerfa, ekki síst með tilliti til krafna sem gilda um öryggi og persónuvernd.

Úr mörgu að velja

Upplýsingakerfunum sem skólar nota má skipta í nokkur mismunandi kerfi, þ.e. kennslukerfi, nemendabókhaldskerfi, innritunar- og umsóknarkerfi, innheimtukerfi, o.m.fl. Sumir skólar nota mismunandi kerfi sem svo tengjast öðrum kerfum. Hér má nefna að fjölmargir framhaldsskólar nota Innuna sem nemendaskráningarkerfi og MySchool eða önnur kerfi til að halda utan um kennsluvef námskeiða. Þannig getur einn skóli notað erlend kennslukerfi og innlent innritunar- og innheimtukerfi. Öll eiga þessi kerfi sameiginlegt að í þeim felst varðveisla persónuupplýsinga og á það fyrst og fremst við sjálf nemendabókhaldskerfin sem geyma einkunnaferla nemenda. Einnig eru geymdar verðmætar persónuupplýsingar í umsóknarkerfum skóla.

Fjölmörg kerfi hafa verið notuð hérlendis síðustu ár. Vinsælustu erlendu kerfin hafa verið WebCT, BlackBoard, Moodle, Angel og Google APPS. Þessi kerfi eiga það sameiginlegt að vera fyrst og fremst kennslukerfi til að halda utan um kennsluvefi námskeiða. Kennarar geta dreift efni í gegnum þessi kerfi, skipulagt námskeið og tekið við efni frá nemendum. Í mörgum þeirra erlendu kerfa sem eru í boði geta kennarar fylgst með heimsóknum einstakra notenda (á ensku „tracking students“) inn á mismunandi síður námskeiðsvefja. Hér er m.a. átt við að kennarar geta skoðað hvort nemendur hafi náð í verkefni eða lesefni, halað niður fyrirlestrum, o.s.frv. Algengustu íslensku kerfin eru MySchool, Námsskjárinn, Uglan, Stefanía, Mentor og Innan. Sum íslensku kerfanna bjóða eingöngu upp á kennsluumhverfi en Uglan og MySchool eru dæmi um kerfi sem halda ekki bara utan um kennsluna heldur einnig nemendaskráningu, kennslumat, umsóknir, o.m.fl. Það er því ljóst að þau eru dæmi um kerfi þar sem mörg undirkerfi tala saman og vinna upplýsingar. Samskipti ólíkra kerfa byggja á Scorm-stöðlum sem þýðir að hægt er að tengja þau við hvaða kerfi sem er og flytja upplýsingar á milli kerfa. Þó er ekki öruggt að öll íslensku kerfin byggi á Scorm-staðlinum líkt og flest erlendu kerfin gera.

Fylgja þarf lögum og reglum

Öll íslensku kerfin eiga það sameiginlegt að í þeim er geymt mikið magn persónuupplýsinga þar sem fyllsta öryggis þarf að gæta. Það er hlutverk Persónuverndar að hafa eftirlit með framkvæmd laga nr. 77/2000 um persónuupplýsingar og persónuvernd. Persónuvernd veitir fyrst og fremst leiðbeiningar, setur almennar reglur og hefur eftirlit með því að lögum sé fylgt. Í undantekningartilfellum er vinnsla persónuupplýsinga leyfisskyld, þ.e. háð leyfi persónuverndar. Vegna þessa ber skólum skylda að fara með persónuupplýsingar í samræmi við lög um persónuvernd.

Lögin þýða einfaldlega að þau kerfi sem skólar nota eru mjög aðgangsstýrð og mismunandi eftir aðgangi hversu miklar persónuupplýsingar notendur sjá. Í raun má skipta notendum sem vinna með persónuupplýsingar í nokkra hópa (tekið mið af starfsmönnum í Háskólanum í Reykjavík): starfsmenn kennslusviðs, stjórnendur, starfsfólk deilda í stjórnsýslu og þjónustu, námsráðgjafar, kennarar og nemendur.

Hvaða persónuupplýsingar þarf að gæta sérstaks öryggis með? Hér er átt við gögn sem tengjast námsferlum, próf og úrlausnir nemenda sem eru vistuð í gagnagrunna og ýmiss konar fylgigögn á rafrænu formi sem nemendur senda með umsóknum. Aðgengi notendahópa er mjög stýrt og geta t.d. deildarfulltrúar í tækni- og verkfræðideild ekki skoðað námsferla nemenda í öðrum deildum. Aðgengi nemenda og almennra starfsmanna er hins vegar bundið við almennar persónuupplýsingar, t.d. nöfn, kennitölur, heimilisföng, símanúmer og myndir, þ.e. ef mynd er til staðar í kerfinu.

Gögn notuð til greiningar

Upplýsingagjöf til hins opinbera hefur færst í vöxt hin síðari ár. Er þá oft um viðkvæmar upplýsingar að ræða sem þarf að kalla fram úr mismunandi kerfum skólanna. Þetta geta verið skýrslur um fjölda nemenda til Hagstofunnar. Þær skýrslur sýna t.d. fjölda lokinna eininga, nám sem viðkomandi er skráður í, innritunardag og útskriftir. Upplýsingar sem Hagstofan óskar eftir eru venjulega fyrir erlendar samanburðarskýrslur, t.d. Education at Glance (gefið út af OECD) og einnig upplýsingar sem þarf að skila EURYDICE og Norrænu hagtölubókinni. Einnig þarf að skila upplýsingum til mennta- og menningarmálaráðuneytis um þreytt próf stúdenta. Aðrar skýrslur sem skólar gegna skilaskyldu á eru skýrsla um starfsfólk til Hagstofu, þá hlutfall kennslu, rannsókna og stjórnunar hjá starfsfólki háskóla, skýrsla um umsækjendur til mennta- og menningarmálaráðuneytis, sérstakar skýrslur sem hið opinbera kann að fara fram á um t.d. fjölda eininga sem atvinnulausir eru að taka í skólum, o.m.fl. Einnig rata oft inn á borð skóla fyrirspurnir frá Alþingi um málefni er varða nemendur, t.d. fjölda fjarnámsnemenda eftir búsetu og tegund náms. Allar þessar skýrslur og fyrirspurnir eiga það sameiginlegt að þær fela í sér vinnslu persónuupplýsinga sem varða lög um persónuvernd. Í samræmi við beiðnir hins opinbera um æ fleiri tegundir upplýsinga ár hvert þá þurfa kerfin sem unnið er með verið í stöðugri þróun til að tryggja að hægt sé að ná réttum upplýsingum út úr þeim á auðveldan og einfaldan hátt. Einungis fáir starfsmenn skóla eiga hafa aðgang að ofangreindum skýrslum og það þarf að vera tryggt að það sama sé við lýði hjá hinu opinbera. Einnig þarf að sjálfsögðu að tryggja að upplýsingarnar séu ekki rekjanlegar á nokkurn hátt.

Þar sem um viðkvæmar upplýsingar er að ræða í upplýsingakerfum þarf afritun gagna að vera í föstu ferli. Það þýðir að taka þarf afrit daglega og geyma í ákveðinn tíma, t.d. 20 daga. Mælt er með að taka fullt afrit (e. full backup) af gagnasvæði einu sinni í viku og geyma það í a.m.k. eitt ár.

Það er ljóst að notkun upplýsingakerfa í skólaumhverfi muni aukast mikið á næstu árum og því er mikilvægt að huga vel að öryggi gagna og hvernig aðgangi er stýrt að þessum kerfum.

Sigmar Jónsson, deildarstjóri tæknisviðs Fjölgreiðslumiðlunar

Þegar rætt er um stuld á greiðslukortaupplýsingum vilja margir horfa á vandamálið sem eitthvað sem gerist erlendis og fólk les um í erlendum miðlum. Þótt stærðargráðan á þeim málum sem upp hafa komið hér á landi sé ekki sú sama og gerist erlendis er vandamálið ekkert minna hér.

Tölvuinnbrot, öryggismál og ábyrgð seljenda

Á síðustu árum hafa erlendir aðilar í auknum mæli reynt að komast yfir greiðslukortaupplýsingar úr kerfum íslenskra söluaðila og hraðbönkum. Fram til ársins 2006 var þetta óþekkt vandamál á Íslandi en síðustu ár hefur þessi þjófnaður aukist mikið. Þær árásir sem gerðar hafa verið hafa sýnt okkur að ef veikleikar uppgötvast eru þeir misnotaðir hratt. Þannig höfðu ekki komið upp svikamál tengd hraðbönkum í nokkur ár en á sjö vikum komu upp þrjú mál sem nýttu sér sama veikleikann. Þessi mál voru vel skipulögð og markmiðið að svíkja út miklar fjárhæðir. Nú er svo komið að innbrot hjá söluaðilum sem notast við kassakerfi er vaxandi vandamál. Öllum söluaðilum sem meðhöndla og/eða vista greiðslukortaupplýsingar ber að uppfylla PCI-DSS öryggisstaðalinn. Þessi staðall var þróaður af VISA, MasterCard, Amex, JCB og fleiri aðilum til að stemma stigu við stuldi á greiðslukortaupplýsingum. Fyrir nær alla íslenska söluaðila er krafa um að gera sjálfsmat fyrir sitt fyrirtæki. Upplýsingar um staðalinn er hægt að lesa á www.pcisecuritystandards.org og á www.kortaoryggi.is

Vandinn er til staðar hér á landi

Þegar rætt er um stuld á greiðslukortaupplýsingum vilja margir horfa á vandamálið sem eitthvað sem gerist erlendis og fólk les um í erlendum miðlum. Þótt stærðargráðan á þeim málum sem upp hafa komið hér á landi sé ekki sú sama og gerist erlendis er vandamálið ekkert minna hér. Áhrif þjófnaðarins á fyrirtæki hér á landi geta verið hlutfallslega jafn mikil og á þau fyrirtæki sem við lesum um í öðrum löndum. Fyrir þá aðila sem sjá um netöryggi er skylda að lesa skýrslu frá Verizon Business sem fjallar um þau innbrot sem þeir rannsökuðu á einu ári. Hægt er að nálgast skýrsluna á slóðinni http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Fjölgreiðslumiðlun (FGM) eyddi nærri 1000 klst. í vinnu tengda rannsóknum á tölvuinnbrotum hjá íslenskum söluaðilum á árinu 2009 og verður hér að neðan fjallað nánar um niðurstöður og hvað má betur fara. Það virðist vera útbreitt viðhorf margra söluaðila að „ekkert þurfi að gera ef ekkert bilar“ þegar kemur að viðhaldi netkerfa. Þetta viðhorf virðist einkennast af þekkingarskorti á nauðsynlegu öryggi og þeirri áhættu sem fylgir meðferð greiðslukortaupplýsinga. Okkar rannsóknir leiddu í ljós að ástand búnaðar versnaði oftast eftir því sem söluaðilarnir voru minni. Mjög stór hluti afgreiðslukassa hafði ekki uppsetta vírusvörn og nær allir afgreiðslukassar leyfðu jafnframt óheftan aðgang að internetinu. Mikið var um illa varinn þráðlausan netbúnað (WiFi) sem hafður er á sama neti og afgreiðslukassarnir. Eldveggir ekki virkjaðir á vélum söluaðila og enginn sem þjónustar netkerfið. Misskilnings gætir hjá söluaðilum að sá aðili sem viðheldur afgreiðslukerfinu sjái einnig um alla aðra þætti er snúa að tölvukerfinu. Jafnframt að afgreiðslukassar séu ekki eins opnir fyrir netinnbrotum og aðrar Windows PC tölvur því þeir eru ekki notaðir fyrir tölvupóst og til að vafra um á internetinu.

Dæmi um innbrot og rannsókn

Til að átta sig betur á umfangi tölvuinnbrots hjá söluaðila er best að setja upp dæmi. Segjum að viðkomandi aðili sé í veitingarekstri og sé með einn afgreiðslukassa sem tekur við greiðslukortum, annan kassa fyrir afgreiðslupantanir og eina bókhaldsvél. Tekið skal fram að söluaðilinn vistar engar greiðslukortaupplýsingar í sínu kerfi. Hann tekur við 3000 færslum á mánuði eða um 10 færslum á klukkustund miðað við 10 tíma opnun á dag. Söluaðilinn fær inn til sín óværu sem gæti hafa komið í gegnum þráðlaust net, „remote“ aðgang eða við netnotkun starfsmanna. Óværa þessi safnar saman kortaupplýsingum í 90 daga áður en misnotkun hefst á viðkomandi kortum. Þegar sviksamlegar úttektir byrja beinist rannsókn málsins að þessum tiltekna söluaðila. Fyrstu viðbrögð eru að greiðsluvirkni í kassakerfi er tekin úr sambandi og posi settur í staðinn til að koma í veg fyrir áframhaldandi leka á meðan á rannsókn stendur. Viðkomandi færsluhirði er skylt að kalla til erlent rannsóknarfyrirtæki til gagnaöflunar og rannsóknar á netkerfi söluaðilans. Ef niðurstaða rannsóknar leiðir í ljós að óværa hlerar greiðslukortaviðskipti í afgreiðslukerfum seljanda og að ekki eru uppfylltir öryggisstaðlar kortasamsteypanna getur seljandi átt von á umtalsverðum fjársektum. Fyrir utan tjón sem seljandi verður fyrir vegna sekta getur seljandi orðið fyrir skertri ímynd ef málið verður opinbert auk þess sem viðkomandi söluaðili getur ekki notað greiðsluvirkni kassans aftur.

Af hverju getur söluaðili ekki móttekið greiðslukort í kassanum aftur? Eftir að gagnaleki í hans kerfi kemur upp verður PCI-DSS úttektaraðili að framkvæma vottun á hans greiðslukortaumhverfi í samræmi við staðalinn. Enginn aðili á Íslandi hefur heimild til að framkvæma slíka vottun. Ferlið er mjög dýrt og kallar á árlegar endurvottanir. Því má segja að auka kostnaður vegna þessa á hverja færslu verði of hár fyrir lítinn aðila.

Hvað má gera til að fyrirbyggja innbrot

Hvað er hægt að gera til að draga úr þessari hættu? Eins og kom fram hér að ofan eiga allir söluaðilar sem miðla og/eða vista greiðslukortaupplýsingar að uppfylla PCI-DSS staðalinn. Hér fyrir neðan verða talin upp nokkur atriði sem ber að skoða strax (í flestum tilfellum ódýrar lausnir).

- Þráðlaus net eiga ekki heima á netkerfi með afgreiðslukössum. Ef nauðsynlegt er að hafa þráðlaus net í fyrirtækinu er best að setja þau upp á sérstaka ADSL línu og ekki tengja við önnur net.
- Afgreiðslukassar þurfa ekki ótakmarkaðan aðgang að internetinu. Þeir þurfa að hafa samband við færslumiðlara, geta sótt uppfærslur fyrir stýrikerfið og vírusvarnir en ekki mikið annað. Ef afgreiðslukassi hefur fullan aðgang að internetinu er auðvelt fyrir óværur sem komast inn að senda upplýsingar út.
- Virkið hugbúnaðareldvegg á öllum tölvum. Það minnkar líkur á að óværa sem kemst inn á eina vél nái að færa sig á aðrar vélar innan netsins.
- Fjaraðgangur (remote) að netkerfi þarf að vera mjög takmarkaður. Ef þjónustuaðilar geta tekið yfir tölvur á netkerfinu þínu án þess að þú opnir sérstaklega fyrir það í hvert skipti ertu að bjóða hættunni heim. Oft eru svona tengingar ekki uppfærðar reglulega og auðvelt fyrir aðila að nýta sér þekkta veikleika í þeim.
- Ekki setja upp hugbúnað á afgreiðslukössum sem ekki er þörf á. Skoða þarf reglulega hvort nýjar uppfærslur hafa komið af viðkomandi hugbúnaði. Því meira af hugbúnaði sem keyrandi er á tölvunni því fleiri veikleikar eru til staðar.
- Nauðsynlegt er að uppfæra kerfis- og veiruhugbúnað reglulega.
- Ef starfsmenn koma með sínar tölvur í vinnuna eiga þær að vera á sér neti sem ekki tengist netkerfi fyrirtækisins. Æskilegast að nota þráðlausa netið sem rætt var um í fyrsta lið.
- Áhættusamt er að notast við USB minniskubba innan netkerfis fyrirtækis ef viðkomandi kubbur er einnig notaður utan þess. Af þeim sökum er hættulegt þegar þjónustuaðilar nota USB kubba til að uppfæra kerfi hjá söluaðilum þar sem sami kubburinn fer á milli margra aðila.
- Þegar nýr aðili tekur yfir fyrirtæki sem meðhöndlar greiðslukortaupplýsingar er nauðsynlegt að láta fagaðila gera úttekt á öllu tölvukerfi fyrirtækisins. Ef þú ætlar að kaupa notaðan bíl ferð þú með hann í gegnum ástandsskoðun, það sama á að gilda um tölvukerfi notaðs fyrirtækis. Nauðsynlegt er í þessu ferli að eyða öllum gömlum gögnum sem ekki er þörf á. Það er mjög slæmt að greiðslukortaupplýsingar fyrri eigenda valdi nýjum eigendum skaða.

Atriðin hér að ofan gera tölvukerfi söluaðila ekki örugg en þau gera ástandið mun betra en það er í dag. Næsta skref er að uppfylla PCI staðalinn með því að standast sjálfsmatið. Sjá nánar kröfur staðalsins á www.pcisecuritystandards.org og á www.kortaoryggi.is

Laufey Erla Jóhannesdóttir, öryggisstjóri hjá Símanum

Óheiðarlegir aðilar nota upplýsingar um einstaklinga til að yfirtaka líf þeirra og svíkja aðra.

Tölvuþrjótar nýta sér veikleika eða galla í hugbúnaði ásamt grunleysi notenda til að ná markmiðum sínum.

Til að gera þrjótunum erfiðara fyrir verður almenningur að verða meðvitaðri og hugbúnaður að vera laus við algenga og vel þekkta veikleika.

Hvernig gerum við tölvuþrjótum erfiðara fyrir?

Mikilvægi internetsins og veflausna

Flestir nota internetið til að sinna ýmsum erindum og telja sig örugga fyrir afskiptum óviðkomandi. Fæstir vita af aukningu netglæpa sem sést hefur undanfarna mánuði. Það er eftir miklu að sækjast á internetinu og nettengdum tölvum. Í hverri tölvu er nú bankaútibú og eiga bæði bankar og notendur erfitt með að tryggja öryggi fjármuna sem fara um netbanka. Persónulegar upplýsingar eru einnig eftirsóttar, sérstaklega í stærri samfélögum þar sem auðvelt er að villa á sér heimildir. Óheiðarlegir aðilar nota upplýsingar um einstaklinga til að yfirtaka líf þeirra og svíkja aðra. Njósnir um fyrirtæki, stofnanir eða ríkistjórnir eiga sér stað einnig stað með aðstoð internetsins og veflausna.

Tölvuþrjótar nýta sér veikleika eða galla í hugbúnaði ásamt grunleysi notenda til að ná markmiðum sínum. Allir hagsmunaðilar sem koma að rekstri veflausna verða að vinna saman gegn tölvuglæpum og bæta öryggi internetsins, þó sumir sem eiga að tryggja öryggið virðist sofa á verðinum. Aðgerðaleysi gæti leitt til þess að fólk missi traust á internetinu og hætti að nota netbanka og netverslanir. Slík þróun ylli miklu óhagræði t.d. ef almenningur hætti að nota netbakana og mætti í útibúin, slíkt myndi hafa veruleg áhrif á bankana.

Þróun tölvuglæpa

Tölvuþrjótar nútímans eru ekki nördar sem stunda iðju sína til að sanna sig. Glæpirnir hafa þróast úr veggjakroti og öðrum skemmdarverkum yfir í háþróuð innbrot og bankarán. Þetta eru atvinnumenn sem hafa yfir að ráða meiri þekkingu og betri búnaði en áður þekkist. Fyrirtæki sem rannsaka tölvuglæpi finna stöðugt ný dæmi um mjög þróaðan hugbúnað og aðferðir sem tölvuþrjótar ráða yfir. Starfsemi sumra tölvuþrjóta er mun agaðri og skipulagðari en margra fyrirtækja. Nú er talið að tölvuglæpir séu hluti af skipulagðri glæpastarfssemi og ágóðinn af þeim jafnvel meiri en af fíkniefnaviðskiptum.

Einnig er talið að ríkisstjórnir og leyniþjónustur noti netið til njósna og hernaðar gegn andstæðingum sínum.

Á stundum virðist þetta vera vonlaus barátta og fátt sem getur stöðvað þróunina. En það er ekki hægt að gefast upp baráttulaust. Til að gera þrjótunum erfiðara fyrir verður almenningur að verða meðvitaðri og hugbúnaður að vera laus við algenga og vel þekkta veikleika.

Þekking er besta vörnin

Til að koma í veg fyrir að almenningur verði fórnarlamb netglæpamanna verður að bæta upplýsingagjöf og auka umræðu. Upplýsingar um hættur og hvernig má forðast þær verða að vera aðgengilegar og opnar öllum hagsmunaaðilum. Vakning um vandamálið þarf að eiga sér stað meðal upplýsingatæknifyrirtækja, menntastofnana og fyrirtækja sem bjóða þjónustu á netinu.

Hádegisfundur Skýrslutæknifélagsins í febrúar 2010 um öryggi og upplýsingar var mjög gott framtak til að vekja athygli á tölvuglæpum og háþróuðum aðferðum tölvuþrjóta. Mikilvægt er að framhald verði á sambærilegum viðburðum og að umræðan leiði til aðgerða bæði meðal notenda, fagfólks og menntastofnana.

Upplýsa verður almenning um hættur á internetinu, aðferðir tölvuþrjóta og hvernig hægt er að nota netið á öruggari hátt. Menntun í upplýsingatækni fyrir almenning verður að breytast, sérstaklega fyrir börn og unglinga.

Bæta verður menntun og þjálfun fagfólks í upplýsingatækni. Endurskoða þarf námsefni og námsframboð þannig að fagfólk fái menntun í forritun og þróun öruggari hugbúnaðar.

Nú er þetta mjög takmarkaður hluti af námskránni ef nokkur. Fyrirtæki í hugbúnaðargerð og rekstri verða að bæta þjálfun og símenntun starfsmanna sinna. Ef fagfólk fær ekki viðeigandi þjálfun og bætir sig, þá munu þrjótarnir hafa betur.

Duldar árásir og nýjar smitleiðir

Tölvuþrjótar nota andvaraleysi notandans og veikleika í hugbúnaði til að komast yfir upplýsingar í tölvu hans eða taka hana yfir. Fjöldi veikleika vex hratt og tíminn sem líður frá því að veikleiki finnst og þar til tölvuþrjótar hafa notfært sér hann styttist.

Niðurstöður öryggisfyrirtækja sýna að helsta dreifingarleið fyrir tölvuóværu er í gegnum sýkt vefsvæði. Árásin á sér stað án þess að notandinn verði nokkurs var. Heimsókn á heimasíðu sem þrjótarnir hafa „lagað til“ nægir. Meðan notandinn skoðar vefsíðuna er óværunni, t.d. troju eða bakdyrum hlaðið niður á tölvuna hans. Um leið og óværan er komin í tölvuna fer hún að vinna fyrir þrjótinn.

Skimanir öryggisfyrirtækja sýna að þrjótarnir sækjast eftir að koma „gildrum“ sínum fyrir á vinsælum heimasíðum. Sérstaklega þeim sem leyfa notendum að setja inn eigið innihald, það auðveldar vinnu þrjótanna til muna. Þetta er ein af ástæðum þess að m.a. Facebook er vinsæl ekki aðeins meðal almennings heldur líka þrjóta. Fjöldi annarra vinsælla heimsíða hefur verið „misnotaður“ af þrjótum og ekkert lát virðist vera á þessum árásum. Óværur sem sérfræðingar hafa „krufið“ hafa reynst mjög fullkomnar, einnig hugmyndafræðin við óværudreifinguna sýna að þekkingarstig og tæknileg færni þrjótanna er mikil. Þetta eru öflugir andstæðingar sem eru erfiðir viðfangs. Þeir eru sveigjanlegir og fljótir að laga sig að breyttum aðstæðum meðan þeir sem verjast eru oft lengi að átta sig á árásinni og koma með lagfæringar.

Það versta við þessa þróun er að veikleikarnir sem þrjótarnir nota sér eru flestir vel þekktir og hægt að komst hjá þeim. Stærsti veikleikinn er ekki í hugbúnaðinum, heldur hjá þeim sem setja upp og sjá um heimasíðuna.

Ábyrgð eiganda

Vefsvæði eða heimasíða samanstendur af mörgum hlutum bæði vélbúnaði og margs konar hugbúnaði. Til að halda úti heimasíðu þarf að minnsta kosti vélbúnað, netbúnað og -tengingu, stýrikerfi, ýmsa miðlara, gagnagrunna, vefþjón og viðmótslag og vefumsjónarkerfi fyrir utan efnið sem ritstjóri vefsins setur inn en það getur innihaldið virka forritahluta. Algengt er að mismunandi aðilar sjái um einn eða fleiri þessara hluta. Einn sér t.d. um vélbúnað, annar um netbúnað, sjá þriðji um stýrikerfið og vefþjóna meðan sá fjórði setur inn efnið. Sá fimmti og síðasti borgar fyrir allt saman.

Í þessu umhverfi getur verið flókið að skilgreina hver ber ábyrgð á hverju. Það er ljóst að sá sem borgar, eða eigandi vefsíðunnar, er sá sem ber endanlega ábyrgð á öryggi hennar og að hún valdi ekki tjóni. Hann ber einnig ábyrgð á að vefsvæðinu sé viðhaldið og það uppfært reglulega til að

Eigendur vefsvæða verða að gera skýrar kröfur til birgja sinna varðandi öryggi og skýra skiptingu hlutverka og ábyrgðar.

Breyta verður aðferðum við þróun veflausna. Skilgreina verður öryggiskröfur strax við hönnun kerfa líkt og aðrar kröfur.

Fagfólk í hugbúnaðargerð verður að geta mætt auknum kröfum um öruggar veflausnir með því að endurmeta og bæta aðferðir og þekkingu sína.

fyrirbyggja að nýuppgötvaðir veikleikar valdi skaða. Eigendur verða að axla þessa ábyrgð og vinna með sínum birgjum í að uppfylla hana.

Eigandinn þarf ekki að framkvæma alla hluti sjálfur. Hann felur öðrum, birgjum sínum að sjá um einstaka þætti, þar með talið að tryggja öryggið og framkvæma uppfærslur. Það er því miður algengt að eigandi vefsíðu veit ekki hvaða ábyrgð hann ber eða hvaða kröfur hann ætti að gera til birgja sinna. Hann treystir því að þeir viti betur en hann og geri hlutina óumbeðið og ókeypis.

Eigendur vefsvæða verða að gera skýrar kröfur til birgja sinna varðandi öryggi og skýra skiptingu hlutverka og ábyrgðar. Það verður að skilgreina í samningum hver tekur ábyrgð á hverju og sér um hvað. Eigendur ættu líka að neita að taka við vöru sem inniheldur þekkta veikleika. T.d. geta menn krafist að vefsíður séu lausar við veikleika sem taldir eru upp í OWASP TOP 10 listanum yfir þekkta veikleika. Meðan kaupendur gera ekki kröfu um ógallaða vöru mun seljandinn ekki bæta sig.

Ábyrgð þeirra sem framleiða og reka heimasíður

Þeir sem þróa veflausnir og heimasíður verða að bæta þjálfun starfsmanna sinna og bæta vinnuaðferðir sínar. Fæstar heimasíður hafa verið hannaðar til að standast árásir. Of margar eru frumgerðir eða tilraunir sem tókust of vel. Þeim var aldrei ætlað að vera á internetinu en áður en nokkur vissi voru þær „óvart“ komnar í loftið. Þetta er sambærilegt við það að gleyma að setja lás í útidyrahurðina.

Meðan hvorki kaupandi eða framleiðandi netlausna taka ábyrgð á öryggismálum aukast hætturnar. Heimasíðan mun innihalda galla sem geta bitnað á eigandanum og þeim sem heimsækja síðuna. Flestar fyrirtækjavefsíður tengjast öðrum kerfum, t.d. lager-, sölu- eða bókhaldskerfi. Gallar í síðunni geta gert þrjótum kleift að komast inní önnur kerfi og sækja úr þeim gögn, breyta gögnum eða eyða þeim. Vitað er um tilvik þar sem þrjótar nýttu sér þekkta veikleika í veflausnum til að stela greiðslukortaupplýsingum frá stórum smásöluaðila og hótelkeðju og ullu tjóni uppá tugmilljónir dollara.

Breyta verður aðferðum við þróun veflausna. Skilgreina verður öryggiskröfur strax við hönnun kerfa líkt og aðrar kröfur. Öryggiskröfum þarf að fylgja eftir í þróunarferlinu frá þarfagreiningu og eftir að lausnin er komin í notkun. Nauðsynlegt er að prófa og skima fyrir þekktum veikleikum á öllum stigum framleiðslunnar og gera reglulega innbrotaprófanir eftir að lausnin er komin í notkun. Það má hvergi gefa afslátt af fagmennskunni þegar veflausnir eiga í hlut. Það verður að beita bestu aðferðum við þróun þeirra eins og alls annars hugbúnaðar.

Mikið hefur verið gert til að til að bæta öryggi hugbúnaðar. Víða má finna gott efni til að auka þekkingu og bæta aðferðir. SAFECode eða The Software Assurance Forum for Excellence in Code eru samtök sem stofnuð voru til að stuðla að auknu öryggi í hugbúnaðargerð. Samtök eins og OWASP og SANS hafa einnig lengi unnið að bættu upplýsingaöryggi. Til dæmis hefur námsframboð í öruggri hugbúnaðargerð hjá bandarískum menntastofnunum batnað mikið vegna þrýstings frá SANS.

Íslensk fyrirtæki og einstaklingar hafa aðgang að öllu þessu efni ókeypis. Það er um að gera að nýta tækifærið og læra að búa til öruggari hugbúnað. Ef menn vilja ganga lengra er mikið framboð af námskeiðum og þjálfun gegn greiðslu. Fyrsta skrefið er þó að ákveða að gera eitthvað í málinu og reyna að bæta sig

Lokaorð

Ein helsta leiðin til að gera tölvuþrjótum erfiðara fyrir er að bæta þekkingu sína með því að skoða efni á áðurgreindum vefsíðum og öðrum síðum með sambærilegu efni. Síðan verða allir hagsmunaaðilar að vinna saman í að gera internetið öruggara. Þyngsta byrðin er hjá eigendum vefsíðna, þeir verða að gera meiri kröfur til birgja sinna um öryggi. Fagfólk í hugbúnaðargerð verður að geta mætt auknum kröfum um öruggar veflausnir með því að endurmeta og bæta aðferðir og þekkingu sína.

Það er á ábyrgð okkar allra að bæta þekkingu okkar og uppfæra samviskusamlega allan hugbúnað sem keyrir á tölvubúnaði sem er á okkar ábyrgð. Ein besta vörnin er að fækka þeim veikleikum sem eru til staðar sem gera þrjótum mögulegt ná valdi á tölvubúnaðinum.

Nytsamar krækjur

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
http://www.sans.org/top25-programming-errors/
http://www.sans.org/top20/2005/spring_2006_update.php
http://www.safecode.org/

Arnaldur Axfjörð, ráðgjafi hjá Admon

Öryggi með rafrænum skilríkjum

Almennt er talið að rafræn skilríki muni gjörbreyta notkun okkar á rafrænni þjónustu. En það gengur ekki eins hratt og vonir stóðu til að innleiða þau hér á Íslandi þannig að notkun sé orðin almenn. Margir velta fyrir sér hvers vegna þetta taki svona langan tíma og sumir skella jafnvel fram fullyrðingum um seinagang og láta í ljós efasemdir um þörf á rafrænum skilríkjum eða notagildi þeirra í samskiptum fólks og í viðskiptum. Það er því ástæða til að setja fram nokkur atriði varðandi rafræn skilríki og uppbyggingu á notkun þeirra á Íslandi, í þeirri von að auka áhuga á rafrænum skilríkjum og efla skilning á notagildi þeirra til að auka öryggi í hinum rafræna heimi.

Hvað eru rafræn skilríki?

Rafrænt skilríki er tölvutækt skjal með upplýsingum um skilríkjahafann og notkunarsvið skilríkisins og inniheldur auk þess gagnastreng sem kallast dreifilykill. Skilríkið er rafrænt undirritað af vottunarstöðinni sem sannvottar útgáfu þess.

Skilríkjunum fylgir einnig leynilykill, svokallaður einkalykill, sem er verndaður í öruggum notendabúnaði þannig að einungis eigandi einkalykilsins, sá sem skilríkið vottar, getur beitt honum. Dreifilykillinn er hins vegar opinber og öllum aðgengilegur. Einkalykillinn og dreifilykillinn eru dulmálslyklar sem eru stærðfræðilega tengdir á ótvíræðan hátt.

Í þessari stuttu grein er ekki ætlunin að lýsa tæknilegri útfærslu rafrænna skilríkja né því umhverfi fyrir útgáfu þeirra og notkun sem kallað er dreifilyklaskipulag, enda eru því gerð góð skil í greininni Almenn útbreiðsla rafrænna skilríkja í 1. tbl. 32. árgangi Tölvumála frá janúar 2007. Auk þess er mikinn fróðleik að finna á vefsetrinu www.skilriki.is.

Uppbygging á PKI Ísland

Unnið hefur verið að uppbyggingu á umhverfi rafrænna skilríkja á Íslandi og notkun þeirra í meira en 10 ár. Tilskipun Evrópuþingsins og -ráðsins nr. 1999/93/EB um ramma ESB fyrir rafrænar undirskriftir var samþykkt 13. desember 1999 og í kjölfarið hófst undirbúningur á lagafrumvarpi fyrir Alþingi sem varð að lögum um rafrænar undirskriftir nr. 28/2001 þann 7. maí 2001.

Ýmsir aðilar á Íslandi buðu fljótlega rafræn skilríki sem byggja á trausti á rótum í eigu stórra fyrirtækja, eins og VeriSign og GlobalSign. Fyrir samfélag eins og Ísland er hins vegar mikilvægt að byggja upp skipulag sem sækir traust í íslenska rót sem er á okkar ábyrgð og sem við höfum fulla stjórn á. Slík „Íslandsrót" skapar það traust sem þarf að vera til staðar í íslensku samfélagi og styður örugg rafræn samskipti almennings, atvinnulífsins og hins opinbera.

Árið 2005 hófst samstarf ríkisins og íslenskra fjármálafyrirtækja um innleiðingu á dreifilyklaskipulagi og almenna notkun rafrænna skilríkja. Dreifilyklaskipulagið hefur verið kallað „PKI Ísland", skammstafað PKI-IS. Þegar drög að skilgreiningu á stefnumarkandi kröfum fyrir útgáfu rafrænna skilríkja lágu fyrir var samstarfssamningur til sex ára undirritaður þann 8. mars 2007. Rúmu ári síðar, þann 20. maí 2008, var Íslandsrót búin til í samræmi við ströngustu kröfur í Evrópu um framkvæmd og öryggisráðstafanir. Íslandsrót er sjálfundirrituð rót og er því uppruni traustsins í umhverfi rafrænna skilríkja sem gefin eru út undir henni.

Í byrjun júní 2008 var milliskilríkið „Fullgilt audkenni", sem er í eigu fyrirtækisins Auðkenni hf., undirritað af Íslandsrót og skömmu síðar var fyrsta rafræna skilríkið gefið út á debetkorti.

Þann 8. október 2008 hófst tilraunaverkefni með stýrðri innleiðing á rafrænum skilríkjum þar sem fyrirhugað var að fjölga skráningarstöðvum markvisst og auka útgáfu rafrænna skilríkja til allra viðskiptavina banka og sparisjóða jafnt og þétt, undir ströngu eftirliti og atvikastjórnun. Skömmu síðar varð ljóst að vegna breyttra aðstæðna hjá bæði ríki og fjármálafyrirtækjum væri ekki forsenda til að halda þeim hraða í uppbyggingu sem væntingar stóðu til. Frá þeim tíma hefur stýrða innleiðingin verið í lágmarki, en þó er búið að framleiða og afhenda nokkur þúsund rafræn skilríki á debetkortum.

Á vormánuðum 2009 var hafin framleiðsla á rafrænum skilríkjum á snjallkortum, svokölluðum starfsskilríkjum, meðal annars til að leysa af hólmi útgáfu Tollstjóra á vefafgreiðsluskilríkjum.

Í samstarfsverkefni ríkis, banka og sparisjóða er því búið að byggja upp dreifilyklaskipulag, mynda Íslandsrót, gefa út stefnureglur, byggja upp stjórnkerfi með ferlum og skipulagi og setja upp öflug áreiðanleg tölvukerfi og framleiðslubúnað fyrir ísetningu skilríkja í örgjörvakort. Þessi uppbygging var mjög umfangsmikil í bæði fjármagni og mannafla, en segja má að varan sé tilbúin og að framleiðslulínan bíði purrandi eftir skipun um að keyra á fullu álagi.

Það sem fyrir liggur er að ljúka uppbyggingu skráningarstöðva í útibúum banka og sparisjóða til að geta afhent skilríkin á ásættanlegan hátt til allra skilríkjahafa. Skráningarstöðvarnar þarf að útbúa sérstaklega með búnaði, aðstöðu og sérþjálfuðu starfsfólki sem sinnir mikilvægu trúnaðarhlutverki. Bankar og sparisjóðir eru mislangt komnir og framundan er töluverð uppbygging hjá sumum þeirra.

Jafnframt þarf að ljúka tilraunaverkefninu í stýrðri innleiðingu og staðfesta að allir þættir í framleiðslu og útgáfu rafrænna skilríkja séu ásættanlegir.

Dreifilyklaskipulagið PKI Ísland

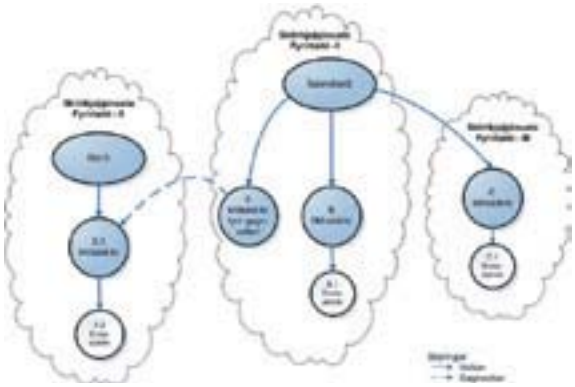
Í örgjörva debetkortanna og annarra snjallkorta sem gefin eru út af Auðkenni eru vistuð tvenn skilríki, önnur fyrir auðkenningu og hin fyrir undirskriftir. Undirskriftarskilríkin eru fullgild skilríki sem kveðið er á um í 7. gr. laga um rafrænar undirskriftir, nr. 28/2001. Þau eru gefin út af vottunarstöð Auðkennis sem fullnægir skilyrðum í V. kafla laganna. Skilríkin eru varðveitt í örgjörva sem telst öruggur undirskriftarbúnaður samkvæmt

Rafrænt skilríki er tölvutækt skjal með upplýsingum um skilríkjahafann og notkunarsvið skilríkisins og inniheldur auk þess gagnastreng sem kallast dreifilykill. Skilríkið er rafrænt undirritað af vottunarstöðinni sem sannvottar útgáfu þess.

Í örgjörva debetkortanna og annarra snjallkorta sem gefin eru út af Auðkenni eru vistuð tvenn skilríki, önnur fyrir auðkenningu og hin fyrir undirskriftir.

ÍSLANDSRÓT

Mynd 1: Merki Íslandsrótar



Mynd 2: Dæmi um skilríkjaútgáfu með trausti á Íslandsrót

IV. kafla laganna. Undirskriftir framkvæmdar með slíkum skilríkjum uppfylla því kröfur um fullgildar undirskriftir í samræmi við lög nr. 28/2001. Þessar kröfur eru samræmdar í Evrópubandalagsríkjunum. Auðkenningarskilríkin eru gefin út á nákvæmlega saman hátt og hafa því mjög hátt öryggistig, þó þau séu ekki ætluð til rafrænna undirskrifta.

Fjármálaráðuneytið rekur vottunarstöð Íslandsrótar. Þar sem Íslandsrót er uppruni traustsins í öllu dreifilyklaskipulaginu þá þarf vottunarstöð Íslandsrótar að uppfylla ströngustu öryggiskröfur allra vottunarstöðva sem undir henni starfa.

Dreifilyklaskipulagið PKI-IS er opið í þeim skilningi að allar kröfur og stefnumið eru öllum aðgengileg og aðilar sem uppfylla stefnumarkandi kröfur PKI-IS geta fengið útgáfuskilríki undirrituð af Íslandsrót. Slík útgáfuskilríki, sem venjulega eru kölluð milliskilríki, má síðan nota til að undirrita endaskilríki fyrir einstaklinga, búnað, félög og fyrirtæki sem skilríkjahafa.

Hvort kom á undan, hænan eða eggið?

En það er ekki nóg að afhenda skilríki til notenda ef þeir geta ekki notað þau. Að innleiða rafræn skilríki er eins og að svara spurningunni um það hvort kom á undan, hænan eða eggið. Væntanlegir handhafar rafrænna skilríkja sjá ekki ástæðu til að tileinka sér rafræn skilríki fyrr en nægjanlegur fjöldi þjónustuaðila býður þjónustu sem byggir á þeim, og þjónustuaðilar eru tregir til að eyða tíma og fjármunum í útfærslu á þjónustu fyrr en umtalsverður fjöldi notenda er kominn með rafræn skilríki. Til að ná árangri þarf því að samstilla uppbyggingu á þjónustu og lausnum sem styðja notkun á rafrænum skilríkjum við dreifingu skilríkjanna til væntanlegra skilríkjahafa. Nú þegar hefur náðst umtalsverður árangur og á vefsetrinu www.skilriki.is er listi yfir 27 þjónustuveitendur sem hafa tekið rafræn skilríki í þjónustu sína. Auk þess er hægt að nota rafrænu skilríkin til innskráningar hjá öllum þeim fjölmörgu aðilum sem nota örugga auðkenningu í sameiginlegu þjónustulagi Ísland.is.

Fullvissustig sannvottunar á kennslum

Rafrænir ferlar og sjálfvirkni í rafrænni þjónustu yfir Internetið gera mismunandi kröfur til sannvottunar á auðkennum, hvort sem þau felast í notendanafni og aðgangsorði, veflykli, einskiptis aðgangsorði (e. one time password), rafrænu skilríki eða öðrum þáttum og samsetningu þátta. Í hverju tilviki fyrir sig þarf að meta áhættu með tilliti til þeirra krafna sem gerðar eru til öryggis og ákvarða kröfur um svokallað fullvissustig sannvottunar á kennslum. Til að samræma viðmið í Evrópu hafa verið settar fram skilgreiningar á fullvissustigum (e. assurance levels) sem ráðast af kröfum til mismunandi þátta sannvottunar, annars vegar við skráningu og afhendingu auðkennanna og hins vegar við beitingu þeirra í sjálfvirkum rafrænum ferlum þegar þörf er á staðfestingu undirskriftar eða á heimildum til aðgangs að gögnum og þjónustu.

Fullvissa við skráningu og afhendingu auðkenna ræðst af þremur þáttum. Í fyrsta lagi af öryggi ferla við sannvottun þess sem fær rafrænu auðkennin. Þar skiptir máli hvort þess er krafist að sá sem er sannvottaður mæti á staðinn, hvernig kennsl hans eru staðfest og hversu mikil vissa er fyrir því að um réttan einstakling sé að ræða.

Í öðru lagi ræðst fullvissustigið af öryggi ferla við útgáfu auðkennanna. Þar skiptir máli hvernig auðkennin eru afhent eða send til handhafans og hvort auðkennin eru afhent í einu lagi eða skipt í hluta sem miðlað er eftir ólíkum leiðum.

Í þriðja lagi ræðst fullvissustigið af öryggi í starfsemi útgefandans við framleiðslu og útgáfu auðkennanna, það er hvort hann uppfyllir tiltekin viðmið og hvort starfsemin er tekin út, vottuð eða á annan hátt staðfest af traustum ytri aðila.

Fullvissa við beitingu skilríkjanna ræðst annars vegar af öryggi auðkennanna sjálfra og hins vegar af öryggisstigi aðferða við sannvottun þeirra. Veflyklar og aðgangsorð sem byggja á fáum bókstöfum eða tölustöfum teljast veik auðkenni, en fullgild rafræn skilríki á hörðum miðli, eins og öruggum örgjörva, eru talin hafa mestan styrk auðkenna.

Mynd 3: Þættir sem hafa áhrif á fullvissustig sannvottunar

Öryggisstig aðferða við sannvottun auðkenna ræðst mest af þeim vörnum sem innbyggðar eru, meðal annars gegn hlerun, stuld á tengilotum (e. sessions) og maður-á-milli (e. man-in-the-middle) innskotum.

Viðmið fyrir fullvissustig eru forsenda fyrir ásættanlegri auðkenningu og

Mynd 4: Merki Skilríki.is

Það sem fyrir liggur er að ljúka uppbyggingu skráningarstöðva í útibúum banka og sparisjóða til að geta afhent skilríkin á ásættanlegan hátt til allra skilríkjahafa.

Með rafrænum skilríkjum opnast möguleikar á nýrri þjónustu sem uppfyllir kröfur um vernd á friðhelgi einstaklinga og varðveislu persónuupplýsinga.

Í STORK koma saman 29 samstarfsaðilar, þar af 14 ríki auk ýmissa fyrirtækja, stofnana og ráðgjafarfyrirtækja.

samhæfingu á milli aðila. Þess vegna er sameiginleg skilgreining á fullvissustigum mikilvæg fyrir samskipti og þjónustu yfir landamæri, t.d. innan Evrópu.

STORK verkefnið

Fjármálaráðuneytið, fyrir hönd Íslands, er aðili að stóru tilraunaverkefni Evrópuþjóða sem kallast STORK. Í STORK koma saman 29 samstarfsaðilar, þar af 14 ríki auk ýmissa fyrirtækja, stofnana og ráðgjafarfyrirtækja. Markmið STORK er að byggja upp sam-evrópskt kerfi fyrir notkun rafrænna auðkenna yfir landamæri. Kerfið byggir á dreifðri högun þar sem settar eru upp samtengdar kerfiseiningar í öllum löndum sem hver fyrir sig þekkir þau rafrænu auðkenni sem notuð eru í hverju landi. Þegar kerfið er fullbyggt þá geta allir borgarar í Evrópu notað þau rafrænu auðkenni sem gefin eru út í þeirra landi til að staðfesta kennsl sín í öðrum löndum.

STORK verkefnið hófst í júní 2008 og lýkur í júní 2011. Þessa dagana er unnið að gangsetningu á fimm markvissum tilraunaverkefnum sem hvert um sig byggir á þjónustuveitum sem nýta sér STORK kerfið fyrir auðkenningu yfir landamæri og miðlun eiginda sem tengjast þeim sem auðkenndir eru.

Fjármálaráðuneytið leiðir eitt þessara tilraunaverkefna sem kallast SaferChat. Markmið með SaferChat er að auka öryggi barna og unglinga í samskiptum yfir Internetið með því að stýra aðgangi eftir aldri og tryggja hæsta öryggi í sannvottun á rafrænum auðkennum. Austurríki og Slóvakía eru samstarfsaðilar Íslands í SaferChat, auk þess sem verkefnið er unnið í samstarfi við Póst- og fjarskiptastofnun, SAFT (Samfélag, fjölskylda og tækni), InSafe sem er stórt verkefni um öryggi barna og unglinga á Internetinu og eTwinning sem er alþjóðlegt verkefni um rafræna fræðslu. Í SaferChat tilraunaverkefninu munu skólar í löndunum þremur vinna sameiginleg verkefni þar sem nemendur búa meðal annars til fræðsluefni fyrir jafningjafræðslu um öryggari notkun Internetsins.

Þessa dagana er verið að ganga frá stækkun verkefnisins þar sem 5 þjóðir bætast í hópinn ásamt fjölda annarra samstarfsaðila.

Í STORK eru sett fram fjögur fullvissustig, svokölluð QAA-stig 1 til 4. Einungis fullgild rafræn skilríki á hörðum miðli, eins og örgjörvum debetkorta og annarra snjallkorta, ná QAA-stigi 4 sem er efsta fullvissustigið. Íslendingar geta því á næstu vikum fengið aðgang að ýmsum þjónustuveitum um alla Evrópu með rafrænu PKI-IS skilríkjunum sínum, enda uppfylla þau STORK QAA-stig 4.

Virðisauki rafrænna skilríkja

Rafræn skilríki hafa mestan styrk allra þeirra auðkenna sem bjóðast í dag, auk þess að vera eina tólið sem uppfyllir kröfur um fullgildar undirskriftir sem kveðið er á um í lögum nr. 29/2001.

Algengast er að nota rafræn skilríki til auðkenninga og til að undirrita rafræn gögn. En með því að nýta eiginleika ósamhverfa lyklaparsins í rafrænu skilríkjunum, fæst í raun fjöldi verkfæra sem nota má til að efla öryggi, auka sjálfvirkni, auka og bæta þjónustu, lækka kostnað, bæta umhverfisvernd og einfalda umsýslu með aðgangi að trúnaðargögnum og að rafrænni þjónustu.

Með rafrænum skilríkjum opnast möguleikar á nýrri þjónustu sem uppfyllir kröfur um vernd á friðhelgi einstaklinga og varðveislu persónuupplýsinga. Einnig er mögulegt að auka verulega rekjanleika aðgerða og miðlunar og fullgera sjálfvirkni í rafrænni þjónustu. Rafræn skilríki geta komið í stað allra annarra aðferða við rafræn kennsl einstaklinga og aðgangsstýringar, svo sem notendanafn og aðgangsorð, einskiptis aðgangsorð (e. one-time-password), veflykla og öryggistalna til staðfestingar á mikilvægum aðgerðum.

Rafræn skilríki einfalda líka verulega umhverfi notenda þar sem sama aðgangsorð, notkunaraðgangsorð skilríkjanna, veitir aðgang að öllum þjónustuveitum. Þar leysa rafrænu skilríkin til dæmis þá þörf sem svokölluð opin auðkenni (e. open ID) eiga að leysa, án þess þó að vera háð viðskiptasambandi þjónustuveitunnar við kennslaveitu (e. identity provider). Það er mikilvægt að hafa í huga að opið auðkenni er í raun ekki auðkenni heldur slóð til kennslaveitu (til dæmis URL) sem getur notað ýmsar aðferðir við sannvottun á kennslum, allt frá veiku aðgangsorði eða veflykli til fullgildra rafrænna skilríkja.

Fullgild rafræn skilríki eru eina verkfærið sem getur myndað fullgilda rafræna undirskrift sem er óhrekjanleg og stendur jafnfætis handritaðri undirskrift fyrir lögum. Rafrænu skilríkin sem gefin eru út undir Íslandsrót eru í fullu samræmi við kröfur, viðmið og staðla í Evrópu. Þau eru því sambærileg við skilríki í öðrum löndum og geta staðfest kennsl yfir landamæri í Evrópu, auk þess sem öllum þjóðum í Evrópusambandinu ber að virða fullgildar rafrænar undirskriftir sem framkvæmdar eru með skilríkjum undir Íslandsrót.

Framtíð rafrænna skilríkja

Í upphafi munu rafræn skilríki mest verða notuð til auðkenningar inn á núverandi þjónustuveitur þar sem auðvelt er að útfæra slíka virkni í vefþjóna og ávinningur notenda er nokkuð augljós.

Hins vegar má búast við því að fljótlega muni þjónustuaðilar bjóða nýja þjónustu sem byggir á rafrænum undirskriftum og því háa fullvissustigi sem rafræn skilríki bjóða. Aðgengi að eigin persónutengdum upplýsingum, jafnvel viðkvæmum upplýsingum eins og heilsufarsgögnum, verður mögulegt. Hægt verður að tengja saman rafræna ferla sem í dag eru rofnir þegar þörf er á staðfestingu á kennslum eða staðfestingu á vilja með undirskrift, og það verður hægt að heimila aðgang með formlegu samþykki ytri aðila eins og þörf er á varðandi aðgang sérfræðinga að ýmsum heilsufarsgögnum.

Rafræn skilríki munu einnig verða notuð til að kalla fram forskráð gögn við afgreiðslu yfir borð. Með því að stinga skilríkjunum í lesara eru auðkenni staðfest samstundis og upplýsingar kallaðar fram úr gagnagrunnum, til að stytta afgreiðslutíma og minnka innsláttarvillur.

Rafræn skilríki verða sjálfsagður þáttur í öllum persónutengdum búnaði, eins og debetkortum, kreditkortum, farsímum og lófatölvum. Öll þessi rafrænu skilríki verða byggð á sömu útfærslu, og til hægðarauka verður hægt að hafa sama notkunaraðgangsorð að þeim öllum, svo fremi sem útfærslan leyfi það.

Hægt er að sækja um rafræn skilríki á debetkorti hjá Arion banka, Landsbanka og Íslandsbanka og á snjallkorti hjá Auðkenni. Nánari upplýsingar eru á vefsetrinu www.skilriki.is.

Svana Helen Björnsdóttir, forstjóri Stika

Þörf hefur skapast fyrir alþjóðlegar reglur um öryggi upplýsinga sem geymdar eru í tölvuskýjum.

Máttur Orðsins

Forsaga

„Í upphafi var Orðið og Orðið var hjá Guði og Orðið var Guð“. Þannig byrjar Jóhannesarguðspjall Biblíunnar. Áður fyrr var upplýsingum miðlað í orðum og orð voru sannarlega mikilvæg, eins og sjá má af upphafi Jóhannesarguðspjalls. Það var ekki fyrr en að Gutenberg fann upp lausa letrið á fyrri hluta 15. aldar að nútíma prenttækni leit dagsins ljós. Oft er sagt að upphaf nútíma prentlistar markist af prentun Gutenbergs á um 120 eintökum af hinni svokölluðu „fjörutíu og tveggja línu Biblíu“. Þetta var árið 1456 og við þessa tækninýjung jukust möguleikar á að miðla upplýsingum og efla þekkingu til muna. Rúmum tveimur öldum síðar voru bækur orðnar nokkuð útbreiddur upplýsingamiðill, en þær voru bæði illa unnar og dýrar.

Fyrstu höfundarréttarlögin litu dagsins ljós í Bretlandi árið 1709. Lögin voru með öðrum formerkjum en þau sem við þekkjum nú og ætlað er að vernda rétt þeirra sem teljast eiga ritverk, hugverk eða aðrar slíkar upplýsingar. Fyrstu lögin voru nefnilega sett sem hvatning til fólks að læra, eða eins og heiti þeirra á ensku ber með sér, „An Act for the Encouragement of Learning“. Þessi fyrstu höfundarréttarlög voru ennfremur sett til að tryggja rétt manna til aðgangs að bókum og upplýsingum, en fram að því höfðu menn getað læst bækur inni og þannig takmarkað aðgang fólks að upplýsingum. Í frönsku byltingunni árið 1789 var síðan gefin út yfirlýsing um réttindi manna sem staðfesti sérstaklega málfrelsi.

Lög til að tryggja málfrelsi voru ekki sett fyrr en undir lok 19. aldar. Fram að þeim tíma var lítil þörf fyrir slík lög, en hún jókst eftir því sem prentun bóka jókst og þær urðu útbreiddari.

Stanslaus flaumur upplýsinga

Nú, þegar upplýsingar flæða rafrænt í stanslausum gagnaflaumi, má segja að tæknin hafi breytt hlutverki ríkis og sambandi þess við borgara sína. Löggjöfin eltir tæknina, en er oft mörgum árum á eftir. Í netkerfum er ekki allt sem sýnist, umfang þeirra nær oft út fyrir sýnilega veggi fyrirtækja og þar af leiðandi eru hin svokölluðu öryggismæri netkerfanna óskýr. Í rauninni eru netkerfin alþjóðleg og upplýsingarnar sem um þau fara samtengjanlegar með ýmsum hætti. Þar sem upplýsingar eru samtengjanlegar alþjóðlega er þörf fyrir alþjóðlegar reglur.

Menn hafa sagt að nú sé upplýsingaöld, en e.t.v. má allt eins segja að nú sé öld óhefts upplýsingaflaums. Enn á ný eru breytingar í miðlun upplýsinga, vinnslu þeirra og vistun. Okkur býðst nú að kaupa upplýsingaþjónustu gegnum þjónustuveitur líkt og rafmagns, hita- og vatnsveitu. Á ensku kallast þetta „Software as a Service“ og skammstafast „SaaS“.

Öryggi upplýsinga á Internetinu

Rekstur tölvukerfa krefst mikillar þekkingar og er afar kostnaðarsamur fyrir marga. Það er hagkvæmara, einfaldara og oft öruggara fyrir mörg fyrirtæki og stofnanir að útvista rekstri tölva og upplýsingakerfa. Einnig á þessu sviði eru breytingar, því nú eru upplýsingar og kerfin sem þær geyma vistuð í svokölluðum tölvuskýjum (e. cloud computing). Kaupandi slíkrar þjónustu veit oft ekki hvar slík þjónusta er staðsett, hann veit jafnvel ekki í hvaða landi upplýsingarnar eru raunverulega geymdar. Það sem meira er, honum er alveg sama svo lengi sem allt virkar sem skyldi.

Tryggja þarf fólki rétt til að sjá upplýsingar sem skráðar eru um það - og rétt til að leiðrétta þær.

Þegar menn vita orðið allt um alla hætta neyðarleg atvik að vera jafn viðkvæm og fyrr.

Það er því ljóst að þörf hefur skapast fyrir alþjóðlegar reglur um öryggi upplýsinga sem geymdar eru í tölvuskýjum. Við mótun slíkra meginreglna þarf að huga að eftirfarandi öryggisþáttum:

- Varðveita þarf leynd upplýsinga þannig að fulls trúnaðar sé gætt.
- Tryggja þarf að upplýsingar séu varðveittar réttar og að þær séu áreiðanlegar, þ.e. að þeim sé ekki breytt á nokkurn hátt né að hluta þeirra sé eytt.
- Upplýsingar þurfa að vera aðgengilegar fyrir notendur með aðgangsheimild, hvenær sem þörf er á.
- Ef færa þarf sönnur á uppruna upplýsinga, þarf að vera unnt að rekja þær til þess uppruna. Slíkt getur átt við fyrir dómstólum í málum er varða persónuupplýsingar, heilsufarsgöng eða fjármálagjörninga.
- Ákveða þarf hvaða vinnsla er leyfð, t.d. hvers konar afritun (dulritun eða ekki), eða samkeyrsla við önnur gögn. Einnig er mikilvægt að skilgreina hvaða vinnsla er óleyfileg.
- Ákveða þarf hvernig er eignarhaldi á upplýsingum er háttað.

Vernd persónuupplýsinga

Persónuvernd er meðal þess sem menn hafa mestar áhyggjur af. Fólk opinberar nú meiri og persónulegri upplýsingar um sig en nokkru sinni fyrr. Óhætt er að segja að samfélagsvefir geri hreinlega út á þetta og tæli fólk til að birta alls kyns viðkvæmar upplýsingar um sjálft sig. Þegar gagnasöfn vaxa og upplýsingamagn um einstaklinga eykst, verður um leið auðveldara að samkeyra slíkar upplýsingar. Upplýsingar geta virst þess háttar að ekki sé hægt að rekja þær til einstaklings, en með hjálp einfaldrar tölvutækni er það nokkuð auðvelt. Við áframhaldandi samtengingu við aðrar upplýsingar um sama einstakling er þannig hægt að afhjúpa hann. Undanfarin ár hafa margir verið hugsi yfir þátttöku í erfðarannsóknum og jafnvel alls ekki viljað láta rannsakendum í té lífsýni sem nota má til að vinna úr erfðaefni. Meðvitund fólks um þær upplýsingar sem falist geta í erfðaefni hefur verið ört vaxandi. Það ríkir hins vegar mikið meðvitundarleysi gagnvart netinu og þeim rafrænu upplýsingum sem víða er safnað um fólk. Rafrænt snið (e. profile) einstaklings sem vinna má úr upplýsingum á netinu getur gefið afar miklar og viðkvæmari upplýsingar um viðkomandi, t.d. ferðir hans, kauphegðun og neyslumynstur.

Segja má að spennuástand hafi skapast milli áhuga einstaklinga á að vernda einkalíf sitt og áhuga fyrirtækja á að nýta sér persónuupplýsingar í viðskiptatilgangi. Hugsanlega má leysa þetta með því að gefa fólki enn meiri aðgang að upplýsingum um sjálft sig og veita því þannig betri stjórn á miðlun upplýsinga um sig. Tryggja þarf fólki rétt til að sjá upplýsingar sem skráðar eru um það, t.d. hjá opinberum aðilum. Sömuleiðis þarf að tryggja fólki rétt til að leiðrétta upplýsingar sem ranglega eru skráðar um það, eða a.m.k. skrá athugasemdir um þær upplýsingar sem fólk telur rangar. Einnig ætti að veita fólki upplýsingar um hverjir hafa séð upplýsingar um það og hvernig, eða í hvaða skyni, upplýsingar um það hafa verið notaðar. Lög og reglur um persónuvernd þurfa að taka mið af þessu og mörgum finnst að persónuupplýsingar þurfi að skilgreina betur sem eign einstaklings.

Internetið - sameign okkar allra

Það er mikilvægt að áreiðanleiki upplýsinga í hinum mikla upplýsingaflaumi sé vel tryggður. Hillary Clinton utanríkisráðherra Bandaríkjanna flutti ræðu um tjáningarfrelsi á Internetinu 21. janúar sl., sjá http://www.state.gov/secretary/rm/2010/01/135519.htm. Þar ávítti hún kínverska tölvuþrjóta fyrir að brjótast inn í tölvur Google. Hún notaði hugtakið „the global networked commons“ og vísaði þar með til þess að Internetið sé hluti af umhverfi okkar eins og hafið eða loftrými. Netið krefjist þar með alþjóðlegs samstarfs til að tryggja sem best skynsamlega, rétta og örugga notkun þess. Ritskoðun eyðileggur netumhverfið. Hún eyðileggur ekki aðeins áreiðanleika upplýsinganna, heldur heftir hún einnig tjáningarfrelsi fólks og kemur í veg fyrir þátttöku þess á vettvangi netsins.

Það er hægt að hugsa sér að stjórnvöld setji reglur um rétta og góða starfshætti við meðferð og vinnslu upplýsinga á netinu, líkt og þau gera varðandi meðferð og merkingu matvæla eða í setningu starfsreglna um almenn heilbrigðismál. Alþjóðaviðskiptastofnunin (The World Trade Organisation) hefur yfirumsjón með frjálsum vöruviðskiptum í heiminum og sú stofnun, eða önnur henni lík, gæti e.t.v. verið viðeigandi aðili til að hafa yfirumsjón með upplýsingaflæði, stafrænum vörum og þjónustu. Það verður hins vegar hvorki auðvelt né þægilegt því til að árangur náist af alþjóðlegu samstarfi á þessu sviði þurfa einstök ríki bæði að samþykkja þátttöku og hafa vilja til að framfylgja reglum um nethegðun.

Endalok einkalífs

Þýska vikuritið Spiegel birti 11. janúar sl. titilgrein sem ber yfirskriftina „Ende der Privatheit“ eða „Endalok einkalífsins“. Í greininni er fjallað á ítarlegan hátt um þær breytingar sem orðið hafa á netnotkun fólks og upplýsingavinnslu allri á undanförnum árum og misserum. Fjallað er um hið stafræna heimsveldi Google, mátt þess og áhrif. Í lok greinarinnar er vitnað til kenninga heimspekingsins David Weinberger um að hin mikla upplýsingasöfnun okkar tíma muni á endanum eyða þeim einkalífsvörnum sem við höfum byggt upp og skapa nýja tegund gagnsæis á menn og málefni. Gagnsæi sem með tímanum muni eyða viðkvæmni okkar fyrir persónuupplýsingum og þeirri spennu sem fylgir verndun persónuupplýsinga. Kenningin Weinberger er sú að þegar menn vita orðið allt um alla hætti neyðarleg atvik að vera jafn viðkvæm og fyrr. Hann spáir því að gegnsæi hins nýja samfélags muni síðan fylgja tími fyrirgefningar, þegar fólk áttar sig á að enginn maður getur nokkurn tíma orðið fullkominn. Þegar allir vita að enginn er fullkominn verði léttara og sjálfsagðara að fyrirgefa.

Lokaorð

Orð það sem ritað er um í Jóhannesarguðspjalli er máttugt og tengist krafti og sköpun. Þau orð sem við venjulega notum til að miðla upplýsingum um okkur og aðra eru ef til vill ekki mjög máttug ein og sér, en þó má ljóst vera að orð og upplýsingar sem í dag er safnað saman til varðveislu um alla framtíð geta sannarlega haft mikil áhrif á líf okkar allra og framtíð. Það verður a.m.k. ekki auðvelt að byrja nýtt líf og ætla sér að hylja fortíðina ef Google og önnur slík fyrirtæki halda áfram að safna öllum upplýsingum um okkur. Það er rétt að gæta varúðar og vanda orð sín á Internetinu því máttur orða á þeim vettvangi er meiri en margir virðast gera sér grein fyrir.

Heimildir:

1. U.S. Department of State: http://www.state.gov/secretary/rm/2010/01/135519.htm
2. Spiegel, Nr. 2/11.1.10, Google - Der Konzern, der mehr über Sie weiß als Sie selbst.
3. The Economist February 27th 2010, a special report on managing information.

Jónas Sturla Sverrisson, CISSP og CISA

Þó svo hægt sé að finna öryggi tölvuskýja allt til foráttu þá þarf maður samt að gera sér grein fyrir því að þau eru komin til að vera í einni eða annarri mynd.

Mynd 1 – hvar eru gögnin?

Öryggið í skýjunum

Hér áður fyrr var vissi maður alveg upp á hár hvar gögn fyrirtækisins voru geymd – annað hvort voru þau á netþjóninum undir borði eða netþjóninum í kústaskápnum. Það var auðvelt að verja gögnin þá.

Í dag er ekki nokkur leið að vita hvar gögnin eru geymd. Þau eru bara einhversstaðar í einhverju skýi og maður nálgast þau bara á næsta kaffihúsi eða í 3G símanum. Allt í einu hefur rekstur á tölvukerfum breyst þannig að núna er borgað fyrir notkun þeirra eins og fyrir notkun á rafmagni eða vatni; allt eftir magni.

Hálfgerð mýri þessi tölvuský

Tölvuský eða á ensku „cloud computing" er hugtak sem hefur misjafna þýðingu í hugum okkar. Tölvuský má segja að sé samheiti fyrir ýmsa eldri tækni sem er vel þekkt t.d. dreifða vinnslu. Nýmælið felst í því að núna er dreifða vinnslan komin á annað stig. Fyrirtækjum gefst kostur á því að leigja sýndarvélar og gagnasvæði allt eftir notkun hverju sinni. Ef þörf er á meiri reiknigetu þá er auðvelt að auka afköstin eða diskaplássið tímabundið. Dæmi um slíka þjónustu eru Amazon S3 og Amazon EC2 og einnig Elastichosts. Stundum er talað um teygjutölvun (e. Elastic computing) sem lýsir þessum eiginleikum vel. Dæmi um aðra tegund tölvuskýja eru aðilar sem bjóða þjónustu eins og afritun, umsjón með samskiptum við viðskiptamenn og skjalakerfi. Fyrirtæki eins og SecurStore, Dropbox, Google Apps og Salesforce bjóða slíka þjónustu. Enn önnur fyrirtæki bjóða upp á vírusskönnun á tölvupósti eins og F-PROT Aves þjónustan gerir. Allt eru þetta dæmi um tölvuský. Ef teiknuð væri mynd af netkerfi fyrirtækis sem nýtir sér tölvuský þá væri útkoman mynd af skýi sem innra net fyrirtækisins tengist við. Annað þyrfti ekki að sýna því það er jú kosturinn við skýin, við þurfum ekkert að vita hvernig þjónustan er útfærð. Í raun eru tölvuskýjum engin takmörk sett. Eitt ský getur nýtt sér þjónustu annarra skýja sem svo gætu nýtt sér enn önnur ský. Það er auðvelt að skilja hvers vegna Ron Rivest hjá MIT vill frekar nota orðið tölvudý (e. swamp computing) fremur en tölvuský.

Ekki alltaf ódýrari valkostur

Með því að nota tölvuský, frekar en eigin tölvubúnað með öllu sem honum fylgir, er hægt að spara talsvert í fjárfestingum en á móti eykst rekstrarkostnaður í staðinn. Í sumum tilfellum er aðeins greitt fyrir notkun en í öðrum fyrir mánaðarlega áskrift. Í könnunum hefur komið í ljós að kostnaður hefur í sumum tilfellum aukist en það hefur verið skýrt með því að ekki hafi verið gerð greining á þörfum áður en farið var yfir í notkun tölvuskýja. Á sama hátt er hægt að benda á fjölda fyrirtækja sem telja sig hafa sparað talsverðar upphæðir á því að nýta sér tölvuský. Sveigjanleiki er mun meiri og auðveldara er að bregðast hratt við breytingum. Einnig er aðgengi mun betra þar sem oftast er hægt að nálgast upplýsingar í tölvuskýjum hvaðan sem er svo lengi sem Internetsamband næst.

Tölvuský hafa ekki slitið barnsskónum ennþá. Þetta er ný hugsun og að mörgu er að hyggja áður en þessi tækni verður orðin betri en það sem við höfum í dag. Mjög mikilvægt er að skoða allar hliðar og rýna sérstaklega öryggið með þrjár megin stoðir þess í huga – leynd, réttleika og tiltækileika. Á mynd 2 má sjá skýringarmynd frá NIST (National Institute of Standards and Technology) um skilgreiningu á tölvuskýjum.

Veikleikar tölvuskýja eru áskorun

Tölvuskýjum fylgja ýmis vandamál sem nauðsynlegt er að gera sér grein fyrir áður en farið er af stað. Þessi vandamál eru af ýmsum toga en stór hluti þeirra tengist upplýsingaöryggi og er því nauðsynlegt að hafa skilning á uppbyggingu þeirra. Markmið tölvuskýja er að gera þjónustu sem þar er boðin ódýra og aðgengilega. Þannig er ljóst að margir viðskiptavinir munu deila með sér tölvubúnaði og diskaplássi ásamt Internettengingu til þess að draga úr kostnaði. Áskorun þjónustuaðilans felst í því að aðskilja með öruggum hætti gögn eins fyrirtækis frá öðrum og tryggja að ekki verði hægt að nýta veikleika í tölvukerfum til þess að ná aðgangi að gögnum og kerfum fyrirtækja í tölvuskýinu. Einnig skiptir miklu máli að aðgangsstýring að þjónustu í tölvuskýinu sé eins örugg og mögulegt er.

Öryggi tölvuskýja

Eftirfarandi atriði ætti að hafa í huga áður en þjónustuaðili er valinn. Þau eru ekki í neinni sérstakri röð og er listinn ekki tæmandi:

- Afritun gagna.
- Neyðaráætlun og áætlun um samfelldan rekstur.
- Lögsagnarumdæmi á geymslustað gagna.
- Hlýting við lög og reglugerðir.
- Örugg eyðing gagna þannig að þau verði ekki aðgengileg aftur.
- Vottun á starfsemi þjónustuaðila.
- Dulritun gagna í fjölnotendakerfi – einn lykill fyrir alla eða einn lykill fyrir hvern viðskiptavin.
- Aðskilnaður milli fyrirtækja í tölvuskýinu.
- Meðferð gagna og kerfa ef þjónustuaðili verður gjaldþrota.
- Réttur til að framkvæma úttektir.
- Úttektir óháðra aðila.
- Tölvuský notar eigin búnað eða búnað í öðru tölvuskýi.
- Meðhöndlun atvika.
- Þjálfun starfsmanna og bakgrunns kannanir.
- Stjórnkerfi upplýsingaöryggis.
- Möguleikar á því að fá dagbókaskrár yfir framkvæmdar aðgerðir.

Mynd 2 - Skilgreining NIST á tölvuskýjum.

Tölvuský má segja að sé samheiti fyrir ýmsa eldri tækni sem er vel þekkt t.d. dreifða vinnslu.

Með því að nota tölvuský, frekar en eigin tölvubúnað með öllu sem honum fylgir, er hægt að spara talsvert í fjárfestingum en á móti eykst rekstrarkostnaður í staðinn.

- Loforð um uppitíma.
- Heilindi eigenda tölvuskýja.
- Örugg auðkenning notenda.

Við val á þjónustu í tölvuskýi þarf að taka tillit til ofangreindra þátta. Sumir þessara þátta bjóða ekki upp á málamiðlanir, þeir verða að vera til staðar. Ef við tökum dæmi af t.d. tryggingafélagi sem hefur áhuga á því að færa vinnslu á hluta eða öllum gögnum yfir í tölvuský þá verða eftirfarandi atriði að vera uppfyllt:

- Staðsetning gagna verður að vera þekkt. Lög um persónuvernd gera kröfur um staðsetningu gagna og geta því hamlað valkostum á tölvuskýjum. Amazon býður t.d. upp á þrjár staðsetningar; tvær í Bandaríkjunum og eina í Írlandi til þess að uppfylla lagalegar kröfur.
- Réttur til að framkvæma úttektir hjá þjónustuaðila er krafa í leiðbeinandi tilmælum nr. 1/2005 frá Fjármálaeftirlitinu. Í þjónustusamningi verður að koma fram að Fjármálaeftirlitinu sé heimilt að framkvæma úttekt á aðstöðu þjónustuaðila. Þetta er nauðsynlegt þar sem t.d. tryggingafélög eru eftirlitsskyld.

Ef annað eða bæði atriðin eru ekki uppfyllt þá getur viðkomandi tryggingafélag ekki nýtt sér þjónustuna. Önnur atriði sem tryggingafélagið hlýtur einnig að skoða varða öryggi gagnanna sjálfra. Er t.d. aðeins einn dulritunarlykill sem gerir þjónustuaðila mögulegt að afkóða gögnin eða fær viðskiptavinur sinn eigin lykil fyrir dulritun?

Ef upp koma mál sem nauðsynlegt er að rannsaka verður að vera möguleiki á því að fá dagbókarskrár yfir aðgerðir notenda. Ekki er víst að þjónustuaðili geti afhent slíkar upplýsingar því allt eins er líklegt að í dagbókarskrá sé að finna upplýsingar um notendur annarra fyrirtækja sem eru að samnýta búnaðinn og erfitt eða jafnvel ómögulegt að aðskilja þessar upplýsingar. Einnig gæti orðið erfitt eða ómögulegt að framkvæma réttarrannsókn (e. Computer forensics) á gögnum eða diskum vegna þess að mismunandi aðilar samnýta búnað og kerfi.

Ofsóknarbrjálæði fyrir lengra komna

Þegar við nýtum okkur þjónustu tölvuskýja þá treystum við því að þau séu rekin af heiðvirðum aðilum með það að markmiði að bjóða upp á góða og örugga þjónustu. Ef ég reyni að setja mig í fótspor óheiðarlegra aðila eða glæpasamtaka þá er þarna komin góð leið til þess að komast yfir gögn. Ég gæti búið til tölvuský sem geymir gögn fyrir einstaklinga og fyrirtæki. Öll gögn eru dulrituð þannig að óviðkomandi geti ekki nýtt sér þau. Það er hins vegar bara einn dulritunarlykill og ég geymi hann. Þannig get ég opnað gögn allra notenda og stolið þeim sem mér finnst vera þess virði. Þeim gögnum get ég svo komið í sölu til þeirra sem gætu nýtt sér þau. Hér gæti verið um kreditkortaupplýsingar, upplýsingar um leynilega vöruþróun eða mikilvæga samninga að ræða.

Það þurfa ekki að vera eigendur viðkomandi tölvuskýja sem eru glæpamenn, það er nóg að starfsmenn þeirra séu það eða í það minnsta móttækilegir fyrir mútugreiðslum. Skipulögð glæpasamtök eru nú þegar búin að finna út að það borgar sig að nota tölvur til að stela, svo af hverju ættu þau ekki að nýta sér þann meðbyr sem tölvuskýin hafa, áður en notendur þeirra eru orðnir nægilega varir um sig, til þess að komast yfir verðmætar upplýsingar?

Lestu skilmála og þjónustusamninga vel

Á mynd 1 má sjá dæmi um það hversu óljós tölvuský geta verið. Fyrirtæki ákveður að nota þjónustu Dropbox til að geyma hluta eða öll gögn sín. Fyrirtækið telur að það sé að nota tölvubúnað Dropbox en í raun er Dropbox að nota búnað frá Amazon fyrir þjónustuna. Þetta er gott dæmi um það hvernig tölvuský nota önnur tölvuský til að gera þjónustuna mögulega. Þess má geta að samkvæmt Dropbox þá eru öll gögn dulrituð með AES-256 dulritunaralgrími. Ekki ætla ég að efast um að dulritun eigi sér stað en það sem er hins vegar umhugsunarvert er að lykillinn að dulrituninni er í höndum Dropbox og þar af leiðandi gætu starfsmenn þess opnað öll gögn sem geymd eru hjá Dropbox. Það gerir það að verkum að notendur verða að sjá um eigin dulritun á gögnum sem þeir geyma hjá Dropbox.

> „…YOU ACKNOWLEDGE THAT USE OF THE SITE, CONTENT, FILE AND SERVICES MAY RESULT IN UNEXPECTED RESULTS, LOSS OR CORRUPTION OF DATA OR COMMUNICATIONS, PROJECT DELAYS, OTHER UNPREDICTABLE DAMAGE OR LOSS, OR EXPOSURE OF YOUR DATA OR YOUR FILES TO UNINTENDED THIRD PARTIES."

Í skilmálum Dropbox kemur fram að Dropbox tekur alls enga ábyrgð á sig gagnvart tjóni sem notandi gæti orðið fyrir t.d. vegna þess að skrá týnist eða kemst í hendur á óviðkomandi. Gögn eru afrituð hjá Amazon og fram kemur að þau séu geymd á austurströnd Bandaríkjanna.

Skýjaborgir verða byggðar

Þó svo hægt sé að finna öryggi tölvuskýja allt til foráttu þá þarf maður samt að gera sér grein fyrir því að þau eru komin til að vera í einni eða annarri mynd. Það þýðir því ekkert að berjast á móti heldur verður að finna leiðir til þess að gera þau örugg. Ýmsir aðilar eru að vinna að stöðlun í tengslum við tölvuský t.d. varðandi samskipti á milli kerfa. Slíkt er nauðsynlegt þegar tengja þarf eina þjónustu við aðra þjónustu í öðru tölvuskýi, t.d. bókhald saman við viðskiptamannakerfi. Lesendum er bent á www.cloudsecurityalliance.org til að kynna sér frekari upplýsingar um öryggi tölvuskýja.

Tölvuský eru áhugaverð í augum tölvuþrjóta. Í skýjunum safnast saman gríðarlegt magn upplýsinga sem spennandi gæti verið að komast yfir. Einnig gætu tölvuþrjótar reynt að stöðva vinnslu með DoS árásum á tölvuský og þar með haft áhrif á rekstur fleiri fyrirtækja í einu í stað þess að ráðast á eitt fyrirtæki í einu.

Áður en farið er af stað verður að skoða kröfur til öryggis. Þær eru misjafnar eftir verðmæti og eðli gagna og kerfa. Án þeirrar skoðunar er alveg óljóst hvort allar nauðsynlegar kröfur eru uppfylltar. Það er vel við hæfi að ljúka þessari grein á upptalningu helstu ógna í tengslum við tölvuský samkvæmt Cloud Security Alliance:

1. Misnotkun eða glæpsamleg notkun á tölvuskýjum.
2. Óöruggir tenglar í hugbúnaði (API)
3. Illgjarnir starfsmenn
4. Veikleiki í fjölnotendakerfum
5. Gagnaleki eða tap
6. Þjófnaður á aðgangi, þjónustu eða tengingu.
7. Óþekktar áhættur.

Við þetta má svo bæta sér íslenskum veikleika en það er rekstraröryggi nettenginga eins og Farice og Danice.


Kristján Ólafur Eðvarðsson og Haukur Þórðarson sérfræðingar hjá Sensa

Staðarnet fyrirtækja byggja á netbúnaði sem sameinar netsamskipti innan fyrirtækis og tengist svo víðnetum bæði Interneti og útibúatengingum.

Öryggismál netkerfa

Veikleikar tölvukerfa er varða öryggismál eru mjög tengd almennu aðgengi notenda að tölvukerfunum. Því eru netkerfin mikilvægur þáttur þegar tryggja á öryggismálin, hvort sem um er að ræða rekstaröryggi eða gagnaöryggi. Til að skyggnast aðeins inn í þennan heim ákvað blaðamaður að ræða við tvo sérfræðinga á þessu sviði. Kristján Ólaf Eðvarðsson og Hauk Þórðarson sem báðir starfa hjá Sensa, en Sensa er átta ára gamalt fyrirtæki með sérhæfingu í tölvunetkerfum og öllu sem að þeim snýr.

Jæja strákar, öryggismál netkerfa hlýtur að vera flókið og viðamikið viðfangsefni?
Já satt er það svarar Haukur, öryggismál netkerfa, sérstaklega þar sem notendur eru margir, spanna mjög marga þætti. Flestir tengja það einungis við Internet tengingar og aðgengi hakkara frá Internetinu, en í dag er það orðið tiltölulega vel þekkt fyrirbæri en hins vegar eru aðrir þættir er þarf að hafa í huga.

Við þurfum því að afmarka umræðuna, ef við höldum okkur við aðgang að tölvukerfum í staðarnetum eru einhver sérstök áhyggjuefni þar, sem snúa að öryggismálum?
Staðarnet fyrirtækja byggja á netbúnaði sem sameinar netsamskipti innan fyrirtækis og tengist svo víðnetum bæði Interneti og útibúatengingum, útskýrir Haukur fyrir okkur. Netskiptar sem eru grunnurinn í slíkum kerfum eru æði oft settir upp samkvæmt gamalli venju. Það er oft látið nægja að þeir skili einföldu sambandi yfir í útstöðvar og þar látið kyrrt liggja. Mjög margir keyra staðarnet frekar opið í dag. T.d ef einhverri tölvu er stungið í samband við staðarnetið, þá hefur hún netaðgang að öllu sem tengist viðkomandi fyrirtæki án þess að uppfylla nein sérstök skilyrði.

Staðarnet á kapli

Nú eru notendur í auknum mæli tengdir yfir þráðlaus net, en algengast eru þó enn kapaltengdar vélar. Hvað eru algengustu vandamálin varðandi aðgengi og stjórnum?
Helstu vandamálin á þessu sviði eru oftast tengd búnaði sem tengdur er inn í kerfin sem hegðar sér óeðlilega eða bilun í búnaði sem veldur umferð sem netið ræður ekki við (e.Denial of Service).

Geturðu nefnt okkur dæmi um hvernig hægt er að koma í veg fyrir að notandi tengi utanaðkomandi skipti í portið á fyrirtækis netskiptinn?
Til þess að koma í veg fyrir þetta getum við til dæmis takmarkað fjölda véla sem mega vera á hverju porti, einnig getum við hlustað eftir svokölluðum BPDU pökkum sem sumir heima netskiptar senda frá sér og lokað portunum ef það gerist. Ef við takmörkum fjölda tækja á bakvið portið þá erum við einnig að koma í veg fyrir MAC flooding árás sem getur valdið því að virkni fyrirtækja netskiptis verður eins og hann sé gamall netdeilir (e.hub).

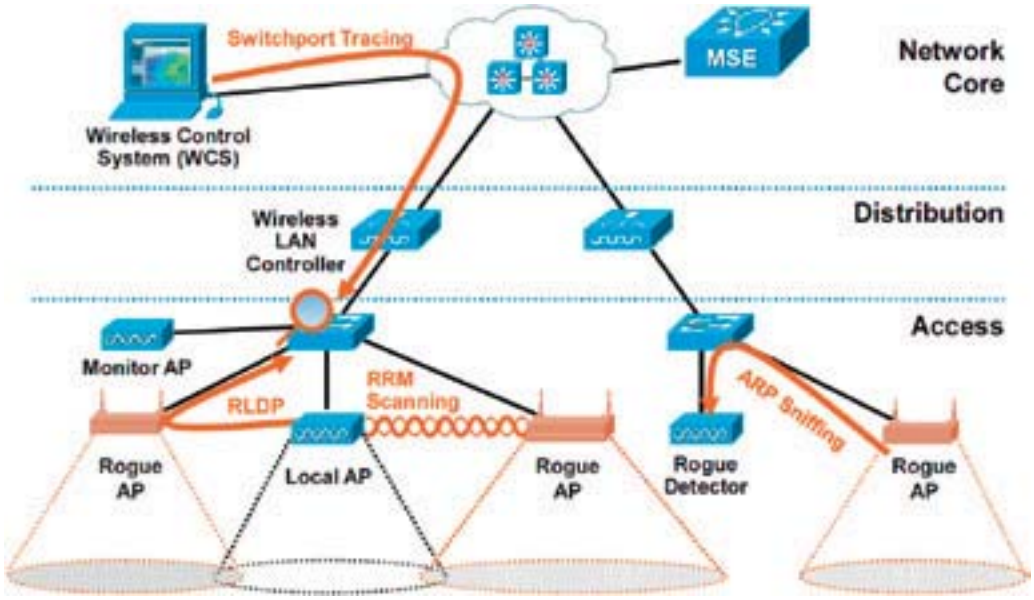
Það hefur oft komið upp að notandi hefur óvart eða viljandi sett sjálfvirka ip tölu úthlutun á staðarnetið og vélar á netinu fá skyndilega rangar ip tölur. Það getur tekið tíma að finna út hvaðan slíkt kemur og slökkva á því. Hvernig er hægt að koma í veg fyrir að það komi fyrir?
Já, þetta hef ég upplifað hjá viðskiptavinum og það er alltaf tímafrekt að finna DHCP þjóninn sem tengdur hefur verið við netið. Sem betur fer erum við komnir með lausn á þessu vandamáli. Ef við virkjum í skiptinum lausn sem kallast DHCP snooping þá komum við í veg fyrir að DHCP netþjónar séu settir upp á notendaportum, einnig takmörkum við DHCP köll sem geta komið frá notandanum og getum líka skráð í DHCP netþjóninn hvar viðkomandi notandi er tengdur inn á netið.

Biluð netspjöld eða vanstilling á multicast valda flóði á netkerfum og hafa valdið því að heilu netkerfin hafa farið á hliðina útaf mikilli umferð. Er hægt að gera eitthvað fyrirbyggjandi þar?
Já, multicast hefur þann kost að það fer á öll tæki á viðkomandi neti sem getur auðvitað snúist gegn okkur þegar þessi traffík verður of mikil og búnaðurinn á netinu hefur ekki undan við að svara þessum fyrirspurnum og hefur þar með kaffært aðra umferð. Þetta er kallað broadcast storm og besta lausnin við þessu er að hanna netin með takmörkuðum „layer 2“ svæðum og skipta netunum upp með L3 skiptum eða beinum. Einnig er möguleiki að takmarka þessa umferð á skiptunum og minnka þar skaðan sem þetta getur valdið.

Hvaða netskiptar styðja þessa virkni sem við höfum verið að ræða um. Getur verið að fyrirtæki séu með þessa netskipta í gangi hjá sér en ekki að nýta sér þessa viðbótar virkni?
Flestir betri fyrirtækjaskiptar sem komið hafa á markaðinn á undanförnum árum styðja þessa möguleika.

Heldurðu að það sé algengt að fyrirtæki séu með búnað í netinu hjá sér án þess að nýta sér þessa innbyggðu virkni?
Á mörgum stöðum er horft á netskipta sem „heimsk“ tæki sem skila einungis umferð frá A-B en ekki hugsað út að þessi tæki geta skilað mun meira rekstrarhagkvæmni með því að koma í veg fyrir óþarfa niðritíma á kerfunum. En nokkrir eru farnir að gera mjög skemmtilega hluti með þessum möguleikum s.s. í kringum DHCP snooping og option 82.

Hvernig stjórnar maður hverjir mega tengjast netskipti og hverjir ekki ?
Já, lausnir í þessum málum hafa verið í mikilli þróun undanfarin ár. 802.1x er lausnin á þessu, þá sendir netskiptir fyrirspurn á auðkennisþjón sem segir hvort viðkomandi notandi hafi aðgang inn á kerfið. Einnig er hægt að nota NAC (Network Addmission Control) tæknina til þess að skoða hvort t.d. vírusvörn og stýrikerfis patchar séu réttir.



Staðarnet yfir þráðlaust samband

Þráðlaus net eru orðin órjúfanlegur hluti af því hvernig notendur eru tengdir við staðarnet fyrirtækja. Þessi notkun gerir notendum kleift að tengjast á fleiri stöðum og þráðlaus net auka framleiðni starfsfólks í fyrirtækjum með t.d minni tíma sem fer í að tengja bæði starfsfólk og gesti á öruggan hátt. Áður en við förum í öryggismálin. Hvernig eru þráðlaus net uppbyggð í dag. Getur stjórnun á stórum þráðlausum kerfum haft eitthvað með öryggismál að gera?

Nútímahönnun á þráðlausum netkerfum byggir á miðlægri stjórnun kerfisins og þar með allra þráðlausra aðgangseininga upplýsir Kristján okkur. Að stjórna mörgum stökum aðgangseiningum í dag er mjög erfitt rekstrarlega séð og tekur of mikinn tíma frá tölvudeildum fyrirtækja. Í dag er flestir að færa sig yfir í miðlægt stjórnunarkerfi sem á engilsaxnesku kallast „Wireless LAN Control". Að hafa kerfi sem er allt stýrt miðlægt tryggir það að hlutir gleymist síður og yfirlitið yfir öryggismálin verður miklu skilvirkara.

Hvað kemur í veg fyrir að notandi eða óprúttinn aðili stingi þráðlausum punkti við staðarnetið til að skapa sér auðveldan aðgang?

Varðandi þetta vandamál, að einhver tengi utanaðkomandi aðgangseiningu í samband við kerfið okkar þá er það vel þekkt í staðarnetum í dag. Cisco og fleiri framleiðendur hafa miðlæga einingu sem kallast Wireless LAN Controller en hann er að „hlusta" á umhverfið og getur þekkt senda sem tilheyra ekki okkar kerfi. Hann getur látið vita ef það eru sendar á netinu okkar sem eru „ólöglegir" og hvort þeir eru tengdir inn á okkar neti eða ekki. Hann getur jafnvel í samspili við netkerfið slökkt á skiptaportinu sem er með ólöglega aðgangseiningu tengda við sig. Einnig er þarna virkni sem lætur þráðlausa netkerfið okkar gera árás á slíka ólöglega senda og aftengja þráðlausu útstöðvarnar af þeim. Við notum þarna í raun þekkta hakkara aðferð til að senda flóð á óvinasendinn og plata svo tölvurnar sem eru tengdar til að tengjast okkur (e. man in the middle attack). Þá látum við notendur aftengjast ólöglega netinu (e. deauthentication), en þetta eru aðferðir sem eru til í dag og eru í notkun víða.

Hvernig tryggjum við að starfsmenn hafi aðgang að þráðlausa fyrirtækjanetinu og hvernig komum við í veg fyrir að utanaðkomandi aðilar tengist netinu?

Er þetta gert með því að setja upp eitt wep-lykilorð eða WPA lykilorð á alla starfsmenn?

Í fyrsta lagi er WEP lykilorðaaðferðin algjörlega ónýt öryggislega séð. Það tekur ekki langan tíma að brjótast inná net með WEP lyklum. Það þarf ekki að vera snjall hakkari til þess heldur eru tól á netinu sem geta fundið lykil að WEP ef það er hlustað á viðkomandi net í einhvern tíma.

Að vera með einhvern einn lykil fyrir alla starfsmenn skalast ekkert sérstaklega vel og er ekki eins öruggt og margir gætu haldið. Sem dæmi ef einhver starfsmaður hættir eða þriðji aðili kemst yfir lykilinn. Til að tækla það þarf þá að breyta lyklinum og þ.a.l á öllum starfsmanna tölvum yfir á nýja lykilinn. Þetta hentar ekki mjög vel í fyrirtækjaumhverfi. En gæti gert það í heimahúsum eða mjög litlum fyrirtækjum.

Er þá einhver betri lausn í boði ?

Já svarið er 802.1x eins og Haukur nefndi. Við notum notendagagnagrunna til að stjórna aðgengi að þráðlausa kerfinu eins og að netskiptunum. Þannig að ef einhverjum notanda er eytt úr grunninum eða hann gerður óvirkur þá hefur þessi tiltekni notandi ekki aðgang lengur, en aðrir notendur haldast óbreyttir.

En hvernig er öryggið á bakvið þetta og dulkóðun sem þú nefnir 802.1x?

802.1x er ekki samskiptastaðall (e. protocol) heldur frekar rammi utan um þessa aðferð sem ég talaði um áðan. Það eru til nokkrar aðferðir til að gera þetta en allar eiga þær það sameiginlegt að 802.1x styður þær. Allar hafa aðferðirnar auðkenningarþjón (e. radius server) og notendagagnagrunn sem þráðlausi sendirinn eða miðlægi stjórnbúnaðurinn (e. wireless controller) tengist við þegar notandinn er að reyna tengingu.

Þekkir þráðlausa miðlæga kerfið einhverjar þekktar árásar hakking aðferðir sem það getur brugðist við?

Já innbyggt í kerfið eru nokkur „árásarmynstur" svipað og fólk þekkir með eldveggi þar sem eldveggurinn þekkir fyrirfram ákveðnar aðferðir og kann að bregðast við þegar hann sér mynstur sem passar. T.d þekkir einn „Wireless LAN Controller" um 17 algengar innbrota aðferðir sem hann getur brugðist við.

Eru ekki fleiri en 17 aðferðir þekktar?

Jú það eru fleiri. Við höfum möguleika að bæta við svokallaðri WIPS þjónustu (e. Wireless Intrusion Prevention) er tengist miðlæga kerfinu. Þarna erum við komin með aukna virkni og getum þekkt og brugðist við yfir 200 árásaraðferðum.

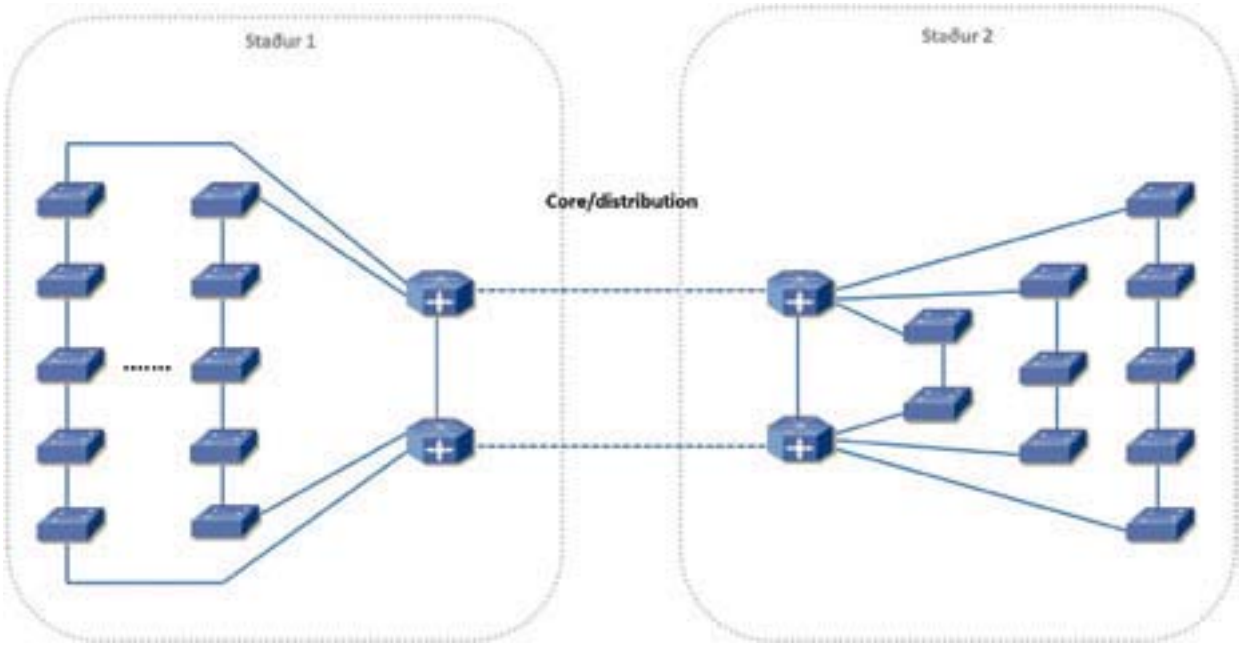
PCI er er vottun sem fyrirtæki sem eru að sýsla með kredit korta upplýsingar gætu þurft að uppfylla. Eru einhverjar kröfur varðandi þráðlaus net sem PCI vottaðir aðilar að vita um?

PCI 1.2 krefst Wips eða skönnunar í raun og veru, jafnvel í umhverfi sem ekki er með þráðlaust kerfi. Það er því erfitt að standast vottunina nema að vera með þráðlaust netkerfi í gangi.

Á mörgum stöðum er horft á netskipta sem „heimsk“ tæki sem skila einungis umferð frá A-B en ekki hugsað út að þessi tæki geta skilað mun meiri rekstrarhagkvæmni með því að koma í veg fyrir óþarfa niðritíma á kerfunum.

Nútímahönnun á þráðlausum netkerfum byggir á miðlægri stjórnun kerfisins og þar með allra þráðlausra aðgangseininga.

Við notum notendagagnagrunna til að stjórna aðgengi að þráðlausa kerfinu og netskiptunum. Þannig að ef einhverjum notanda er eytt úr grunninum eða hann gerður óvirkur þá hefur þessi tiltekni notandi ekki aðgang lengur, en aðrir notendur haldast óbreyttir.



Gestaaðgangur: Mjög algeng krafa er að gestir þurfa internet aðgang. Er gesturinn tengdur við netkerfi líkt og starfsmenn?
Þetta er rétt, þetta er mjög algengt í dag. Ég er ekki sammála því að það sé sniðugt að gesturinn hafi aðgang að staðarneti fyrirtækisins. Í fyrsta lagi er tölva gestsins óþekkt. þ.e hvernig er hún sett upp, hvernig er vírusvörnum háttað eða öðrum tengdum málum. Við erum stundum með viðkvæm gögn á innranetinu sem erfitt er að tryggja fyrir óþekktum aðilum á netinu okkar. Að setja hvern og einn inná okkar net þýðir vinna í hverri heimsókn fyrir tölvudeildir. Það þarf að stilla tölvu hjá gestinum með réttum öryggisstillingum o.s.frv. Þetta getur tekið langan tíma fyrir hvern gest.

Er einhver öruggari og fljótvirkari leið til að leysa þetta?
Já það er til gesta lausn í t.d miðlæga umhverfinu. Þetta virkar þannig að við erum að auglýsa aðskilið gestanet í þráðlausa kerfinu okkar. Þetta er net sem er opið fyrir gesti en er aðskilið frá innranetinu og kemur útá sér hlutlausu (e.DMZ) svæði á eldvegg viðkomandi fyrirtækis. Þannig erum við að verja gestina gagnvart Interneti auk þess sem þeir eru aðskildir frá innrinetum fyrirtækis.

Ef netið er opið. Er þá ekki vandamál að fleiri óviðkomandi geti notað tenginguna?
Þetta er lykilatriði. Við erum með opið net þar sem tölvan þarf ekki að gera neinar öryggisstillingar. Tölvan fær ip tölu en kemst ekkert útá internetið fyrr en notandinn opnar netvafra. Og þarna tekur t.d miðlæga stjórneiningin á móti notendanum með vefsíðu í https og biður um gestaaðgang og lykilorð. Notandinn fær notendanafn og lykilorð fyrir þessa heimsókn (þetta er kóðað með https þegar notandinn sendir það) og þá fær hann internet aðgang.

Og hefur hann þá endalausan aðgang hvenær sem hann vill?
Þetta er góður punktur. En í raun er þetta þannig að notandinn fær tímbundinn gestaaðgang. Aðgangurinn eyðist sjálfkrafa þegar heimsókn er lokið. Það er mjög mikilvægt því þá er gestanetið lokað þegar enginn á að vera að nota það.

Þurfa þá ekki tölvumenn fyrirtækisins að vera uppteknir við að stofna þessa notendur?
Kerfið er yfirleitt hönnuð með svokallaðan „lobby admin“ eiginleika. Þetta er einfaldur aðgangur fyrir t.d þá sem eru í móttöku eða sjá um fundarherbergi fyrirtækja. Þeir skrá sig inná kerfið sem slíkur notandi og geta þar stofnað gestanotendur og eru þannig ábyrgir fyrir sínum gestum og tölvudeildin þarf ekki að koma nálægt því.

Það var greinilega af nógu að taka hjá þessum tveimur herramönnum en það er ljóst að einhvers staðar þurfti að stoppa en við vonumst eftir að heyra frá þeim síðar.

Gyða Halldórsdóttir, M.S. í upplýsingatækni á heilbrigðissviði

Persónuverndarlögin voru sett með það að markmiði að tryggja meðferð persónuupplýsinga við alla vinnslu og vörslu persónu- og trúnaðarupplýsinga.

Öryggi trúnaðarupplýsinga

Þekking, viðhorf og fræðsla

Upplýsingaöryggi er undirstöðuþáttur í nútíma upplýsingatækni sem meðal annars byggir á vandaðri umgengni og vörnum gegn mannlegum mistökum. Öll vinnsla persónugreinanlegra trúnaðarupplýsinga er háð fyrirmælum laga og reglugerða því persónuvernd varðar alla og öryggi rafrænna upplýsinga er alltaf mikilvægt. Magn persónu- og trúnaðarupplýsinga er nú ört vaxandi í gagnabönkum, upplýsingakerfum og á netsíðum opnum almenningi, um leið og þeim sem meðhöndla viðkvæmar persónuupplýsingar fer fjölgandi. Vönduð umgengni og varnir gegn mögulegum ógnum upplýsingaöryggis verða því æ brýnni, þó tæknilegum möguleikum til að tryggja öryggi upplýsinga fleygi ört fram. Árangurinn byggist í grundvallaratriðum á viðhorfi og þekkingu þeirra sem hafa með vinnslu upplýsinganna að gera. Mannlegir þættir upplýsingaöryggis verða hér til umfjöllunar en tækni og tæknibúnaði sem tengist upplýsingaöryggi verða ekki gerð skil.

Kröfur um öryggi persónu- og trúnaðarupplýsinga

Öll vinnsla persónu- og trúnaðarupplýsinga lýtur ákvæðum laga um persónuvernd og meðferð persónuupplýsinga (nr. 77/2000) og einnig laga um réttindi sjúklinga (nr. 74/1997) þar sem það á við. Kröfur eru um að öllum almennum skilyrðum um vinnslu upplýsinga sé fullnægt, gæði og áreiðanleiki upplýsinganna tryggður og sömuleiðis skilyrði um vinnslu viðkvæmra upplýsinga (1; 2). Persónuverndarlögin voru sett með það að markmiði að tryggja meðferð persónuupplýsinga í samræmi við grundvallarsjónarmið um persónuvernd og friðhelgi einkalífs með skilgreindum kröfum um upplýsingaöryggi við alla vinnslu og vörslu persónu- og trúnaðarupplýsinga. Tilmæli landlæknis taka svo sérstaklega á þáttum er varða öryggi sjúkragagna í tölvum (1; 3).

Starfsmenn stofnana/fyrirtækja sem hafa með persónuhætti fólks að gera bera ábyrgð á að tryggja upplýsingaöryggi að viðhöfðum trúnaði og vönduðum starfsháttum. Viðkomandi stofnunum/fyrirtækjum er skylt samkvæmt reglugerð um öryggi persónuupplýsinga (nr. 299/2001) að gera reglulega öryggisráðstafanir sem fyrirbyggja og takmarka tjón af völdum mannlegra mistaka eða misnotkunar. Mikil áhersla er þar lögð á starfsmannamál, ekki síst í þeim tilgangi að tryggja lögmætan aðgang, eðlilega leynd, gæði og áreiðanleika við vinnslu upplýsinganna. Ber þar helst að nefna feril starfsmanns, þagnarskyldu, skilgreiningu hlutverks og aðgang að upplýsingum í samræmi við ábyrgð og starfsskyldur (4).

Vinnslu persónu- og trúnaðarupplýsinga fylgir sú ábyrgð að móta og setja skýra stefnu um upplýsingaöryggi með mælanlegum markmiðum um samfellt aðgangs- og rekstraröryggi upplýsinga. Markmiðið er að upplýsingaöryggi sé tryggt með samfelldum rekstri upplýsingaeigna og reglulegu eftirliti með öllum öryggisráðstöfunum. Eftirlitinu ber svo að fylgja eftir með skriflegu áhættumati um hvað mögulega gæti farið úrskeiðis við vinnslu og vörslu upplýsingaeigna, áhrifum þess og líkum, ásamt umfangi mögulegra ógna og afleiðinga (4).

Þekking, viðhorf og fræðsla

Mikilvægi trúnaðar og ábyrgðarskyldu starfsmanna verður seint fullmetið þrátt fyrir framþróun tæknilegra ráðstafana. Magn persónu- og trúnaðarupplýsinga er ört vaxandi, eins og áður sagði og því hætt við að aukið fyrirliggjandi magn upplýsinga skapi dofa gagnvart trúnaði og mikilvægi þess að vanda alla umgengni um trúnaðarupplýsingar. Það er ekki ofsagt að upplýsingaöryggi stendur og fellur með hollustu og vandaðri umgengni starfsmanna. Reglulegt eftirlit með vönduðum starfsháttum stofnana/fyrirtækja eru þess vegna nauðsynlegir þættir til að tryggja öryggið. Það sem einu sinni hefur gerst getur alltaf gerst aftur. Það er mikið í húfi og vert að nota reynsluna sem víti til varnaðar.

Forsendur þess að öryggisstefna stofnana/fyrirtækja virki og beri tilætlaðan árangur er eindreginn og sýnilegur stuðningur yfirmanna og ábyrgðaraðila við framkvæmd stefnunnar. Skuldbinding starfsmanna gagnvart starfsskyldum, trúnaði og upplýsingaöryggisstefnu í upphafi starfs og með reglulegri ítrekun eru meðal ráðstafana sem eiga að tryggja eðlilega leynd upplýsinga, lögmætan aðgang, áreiðanleika og gæði. Til að fyrirbyggja tjón af völdum mistaka og misnotkunar er nauðsynlegt að hver og einn þekki ógnir við upplýsingaöryggi. Þekking starfsfólks er því mjög mikilvæg í þessu samhengi og vert er að vekja athygli á nauðsyn fræðslu sem stuðlar

Vinnslu persónu- og trúnaðarupplýsinga fylgir sú ábyrgð að móta og setja skýra stefnu um upplýsingaöryggi með mælanlegum markmiðum um samfellt aðgangs- og rekstraröryggi upplýsinga.

Það er ekki ofsagt að upplýsingaöryggi stendur og fellur með hollustu og vandaðri umgengni starfsmanna.

að jafnvægi öryggis og áhættu. Hollusta og viðhorf starfsfólks þróast með þekkingu og hefur áhrif á daglega umgengi við vinnslu trúnaðarupplýsinga og ekki síður tilfinningu fyrir áhrifaþáttum upplýsingaöryggis (4).

Persónuvernd gerir kröfur um fræðslu starfsfólks strax á fyrsta mánuði starfs, með sérstakri áherslu á ábyrgðarskyldu gagnvart upplýsingaöryggi og trúnaði. Fræðslu og þjálfun ber að skipuleggja strax við ráðningu hvers starfsmanns með reglulegri umfjöllun um starfsskyldur og afleiðingar öryggisbrota (4). Starfsmenn eiga að þekkja og vera meðvitaðir um hættur sem ógna upplýsingaöryggi. Staðreyndin er, að upplýsingar sem einu sinni fara út verða ekki aftur teknar. Vert er að nefna hér nokkra þætti sem ógna leynd upplýsinga svo sem blekkingu fólks, meðferð aðgangsorða (leynd, felustaðir), netmiðla (tölvupóst, netsíður og tengla), lausa miðla (minniskubba, geisladiska, vasatölvur, fartölvur og flakkarar) og umgengni við vinnustöðvar (læsing tölva) og prentara (vöktun útprentaðra gagna) (5).
Aðgangsstýringarstefna er einn þáttur upplýsingaöryggisstefnu og er hún nauðsynleg til að tryggja trúnað og persónuvernd (4). Starfsmenn eiga að þekkja reglur um aðgang og aðgangsorð og vera meðvitaðir um hættur á öryggisbrotum. Aðgangsstýringin getur ekki náð tilætluðum árangri nema hver einstaklingur haldi leynd gagnvart öðrum. Þessi öryggisþáttur er ekki einkamál hvers og eins heldur sameinað átak allra. Ein megin reglan er að skilja upplýsingar um eigin aðgangsstýringu aldrei eftir á glámbekk eða öðrum sjáanlegar. Starfsmenn eiga eingöngu að hafa aðgang að gögnum sem eru nauðsynleg vegna starfsins og þeir bera alfarið ábyrgð á hvaða upplýsingar þeir skoða. Aðgang hvers starfsmanns þarf að skilgreina með skýrum hætti og takmarka miðað við hlutverk, eins og áður kom fram. Aðgangur að upplýsingum þýðir ekki endilega umboð viðkomandi til að skoða eða nota upplýsingarnar (4).

Rekjanlegur gagnaferill er hugbúnaður sem skráir inngöngu og alla virkni sem á sér stað í rafrænum upplýsingakerfum, svo sem auðkenni notenda, skrár, dagsetningu og tímasetningu aðgangs og hvað gert er. Rekjanlegur gagnaferill er lykilþáttur í innra eftirliti stofnana/fyrirtækja sem hafa með vinnslu persónuupplýsinga að gera og hefur þann tilgang að hægt sé að ganga úr skugga um virkar öryggisráðstafanir og fylgni við gildandi lög og reglugerðir. Hugbúnaðurinn segir skýrt til um hvað gerðist, hvenær það gerðist og hver framkvæmdi hvaða verknað (5).

Mannlegur máttur

Vert er að huga að viðhorfum og viðbrögðum starfsmanna gagnvart öryggismálum. Hvernig bregðast þeir við? Um það verður ekki fullyrt hér, hvorki góða siði né slæma, en mannlegur máttur getur skipt sköpum í þessu samhengi. Starfsmenn vilja og þurfa aðgang að gögnum, þeir þurfa jafnvel að deila þeim með öðrum og þá skiptir líka sköpum að gögnin séu eingöngu ætluð þeim sem þau þurfa vegna starfsins. Það er auðvelt að deila og dreifa gögnum með þeirri tækni sem býðst í dag. Reglulegt eftirlit og fræðsla eru því nauðsynlegir þættir til að tryggja fylgni við öryggisstefnu. Stundar ábyrgðarleysi, hugsunarleysi eða jafnvel kæruleysi er nóg til að gögnin dreifist og þar með er skaðinn skeður. Kæruleysi eins varðar alla aðra.
Hér hefur verið fjallað um persónu- og trúnaðarupplýsingar óháð því hvers kyns upplýsingar um ræðir. Það er með vilja gert að aðgreina ekki heilbrigðisupplýsingar og aðrar persónu- og trúnaðarupplýsingar. Viðkvæmar persónuupplýsingar eru skilgreindar sérstaklega í lögum um persónuvernd og þær ber að meðhöndla samkvæmt því. Heilbrigðisupplýsingar flokkast þar undir en það á líka við um ýmsar aðrar persónugreinanlegar trúnaðarupplýsingar sem snerta einkahagi fólks eins og upplýsingar um uppruna, kynþátt, stjórnmála-, trúar- og aðrar lífsskoðanir, stéttarfélagsaðild, dóma og kynhegðun. Það er því skýrt að allar persónugreinanlegar trúnaðarupplýsingar skulu meðhöndlaðar sem viðkvæmar trúnaðarupplýsingar (1). Þetta styður ótvírætt að leggja beri áherslu á ábyrgðarskyldu allra sem meðhöndla persónu- og trúnaðarupplýsingar í starfi sínu, hvort sem um er að ræða heilbrigðisupplýsingar eða aðrar viðkvæmar persónuupplýsingar.

Nauðsyn þess að tryggja þekkingu og færni þeirra sem starfa við rafræna umsýslu viðkvæmra trúnaðarupplýsinga er algild. Bretar settu fram hina svo nefndu „Caldicott Guardian“ reglu með ákveðnum lykilatriðum sem ávallt ber að hafa í huga í umgengni persónugreinanlegra trúnaðarupplýsinga. Tilgangurinn var að tryggja viðeigandi umgengni við persónugreinanlegar trúnaðarupplýsingar. „Caldicott Guardian“ reglan byggir á sex mats- og minnisatriðum fyrir alla sem hlut eiga að máli og eiga því vel við hér til áréttingar (6).

„Caldicott Guardian“

REGLUR SEM ÁVALLT BER AÐ HAFA Í HUGA
Í UMGENGNI VIÐ PERSÓNUGREINANLEGAR TRÚNAÐARUPPLÝSINGAR:

1. Rökstuddur tilgangur með umgengni og/eða notkun upplýsinga
2. Notkun upplýsinga eingöngu þegar nauðsyn krefur
3. Notkun á minnsta mögulegu magni upplýsinga
4. Aðgangur að upplýsingum miðað við þarfir
5. Meðvitund um eigin ábyrgðarskyldu
6. Lagaleg stoð fyrir hverri notkun og skýrt hver er ábyrgur fyrir að farið sé að lögum

ECDL Health

Fræðsla og þjálfun þeirra fjölmörgu sem starfa við rafræna umsýslu persónugreinanlegra trúnaðarupplýsinga er brýnt átaksverkefni hér á landi. Aðgengilegt náms- og lesefni um þennan veigamikla málaflokk hefur ekki verið fyrirliggjandi og skort tilfinnanlega. Upplýsingasöfnun og færsla sjúkraskrár eru yfirgripsmiklir þættir í ábyrgðarskyldu heilbrigðisstarfsmanna. Þeim ber að tryggja skjólstæðingum sínum sjálfsákvörðunarrétt og virðingu fyrir mannhelgi með öruggri vörslu og meðferð heilbrigðis- og trúnaðarupplýsinga. Upplýsingatækni og notkun heilbrigðisupplýsingakerfa er lífæð nútíma heilbrigðisstarfsemi.

ECDL Health er heilbrigðishluti evrópska tölvuökuskírteinisins, ECDL (European Computer Driving Licence) eða ICDL (International Computer Driving Licence), sem staðfestir almenna tölvukunnáttu samkvæmt námsáætlun og viðurkenndu prófi. Bretar, Ítalir, Bandaríkjamenn og Finnar hafa komið á viðkenndri fræðslu með prófi (staðfærðu í hverju landi fyrir sig) samkvæmt hugmyndafræði ECDL Health (7). Fleiri þjóðir eins og Írar og Kanadamenn hafa einnig komið á skipulagðri fræðslu og námsferli í sama tilgangi sem fljótt á litið virðist kjörin fyrirmynd. Þeir hafa meðal annars þróað kennslukerfið HITS (Health Informatics Training System), upplýsingatækni í heilbrigðisþjónustu, með fræðslu í mismunandi einingum og prófum sem fara fram á netinu (8; 9). Það sem meira er og góð tíðindi fyrir alla sem hafa með persónugreinanlegar trúnaðarupplýsingar að gera, þá hefur írska upplýsingatæknifélagið ICS (the Irish Computer Society) komið á fót fræðslu og þjálfun í gagnavernd, í samræmi við lög um upplýsingaöryggi, fyrir alla sem vinna með persónugreinanlegar trúnaðarupplýsingar og bjóða þar bæði eins dags inngangsnámskeið og þriggja daga verklega þjálfun á landsvísu (9).

Viðkvæmar persónuupplýsingar eru skilgreindar sérstaklega í lögum um persónuvernd og þær ber að meðhöndla samkvæmt því.

Heilbrigðisráðuneytið, Heilsugæsla höfuðborgarsvæðisins og Skýrslutæknifélag Íslands (SKY) sem er leyfishafi ECDL á Íslandi, voru aðilar að verkefni um vinnslu og útgáfu kennsluefnis og viðurkennds prófs samkvæmt námsáætlun og hugmyndafræði ECDL Health, þar sem til stóð að nota það sem grunn að skipulögðu námsferli ECDL Health á Íslandi. Undirrituð var starfsmaður þessa verkefnis sem var kostað af heilbrigðisráðuneytinu og lauk í ágúst 2008. Formleg ákvörðun hefur ekki verið tekin í heilbrigðisráðuneytinu um að námsferli samkvæmt hugmyndafræði ECDL Health verði tekið upp á Íslandi (11). Hvaða leið verður farin breytir engu um það að fræðsla og þjálfun í gagnavernd og rafrænni umsýslu persónugreinanlegra trúnaðarupplýsinga er og verður brýnt átaksverkefni hér á landi. Nýjar leiðir gefa aukið svigrúm, ekki síst til að fræðsla og þjálfun í gagnavernd verði tekin upp fyrir alla sem vinna með persónugreinanlegar trúnaðarupplýsingar. Ástæðulaust er að byggja aðferðafræðina upp frá grunni þegar fyrirmyndir eru nægar í nálægum löndum. Fyrirliggjandi kennsluefni hjá heilbrigðisráðuneytinu er grunnur sem sjálfsagt er að nýta og reynsla annarra þjóða er einnig mikilvæg í þessu samhengi. Bretar og Ítalir voru til að mynda mjög hjálplegir þegar verkefnið var unnið hér á sínum tíma. Írska upplýsingatæknifélagið hefur verið öflugt á þessu sviði og má mikið af þeim læra sem fyrirmynd (10). Mikilvægast er að hafist verði handa við að efla fræðslu til að auka þekkingu þeirra sem vinna með persónugreinanlegar trúnaðarupplýsingar. Grundvallarþættir sem tryggja viðeigandi skilning og viðhorf gagnvart persónuvernd og trúnaði eru þar forgangsverkefni til framtíðar.

Heimildaskrá

1. Lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000, I.kafli, 2.gr., 4. http//www.althingi.is. [Á neti] 23. maí 2000. [Tilgreint: 23. apríl 2010.] http://www.althingi.is/lagas/nuna/2000077.html.
2. Lög um réttindi sjúklinga. http://www.althingi.is. [Á neti] 28. maí 1997. [Tilgreint: 23. apríl 2010.] http://www.althingi.is/lagas/nuna/1997074.html. 28/1997.
3. Öryggi sjúkragagna. Landlæknisembættið. [Á neti] apríl 2000. [Tilgreint: 25. apríl 2010.] http://www.landlaeknir.is/?PageID=87.
4. Reglur um öryggi persónuupplýsinga. Stjórnartíðindi. [Á neti] 10. apríl 2001. [Tilgreint: 25. apríl 2010.] http://www.stjornartidindi.is/Advert.aspx?ID=1bf932ee-8138-41dd-b7c7-d1b2ace6caa1. 10/2001.
5. Abdelhak, M., Grostick, S., Hanken, M.A. og Jackobs E. (Ritstjórar). Health Information: Management of a Strategic Resource (2. útgáfa). Philadelphia : W.B. Saunders Company.
6. Tameside. Single Assessment Process. Caldicott Principles. Tameside.gov.uk. [Á neti] Tameside, 28. nóvember 2005. [Tilgreint: 25. apríl 2010.] http://www.tameside.gov.uk/sap/principles.
7. EDCL Foundation. EDCL Foundation. EDCL / ICDL Health. [Á neti] EDCL Foundation, 2010. [Tilgreint: 25. apríl 2010.] http://www.ecdl.com/programmes/index.jsp?p=764&n=765.
8. ICS Skills and Health Informatics Society of Ireland. HITS, Health Informatics Training System. ICS Skills. [Á neti] ICS Skills. Training and Certification, 2010. [Tilgreint: 10. maí 2010.] http://ics-skills.ie/hits_about.aspx?sm=95.
9. The Health Informatics Society of Ireland and the Irish Computer Society. Fronline Informatics Training. HITS - Health Informatics Training System. [Á neti] Frontline Informatics Training Inc. [Tilgreint: 20. maí 2010.] https://www.frontlineinformatics.ca/register.php.
10. ICS - Irish Computer Society. ICS - Irish Computer Society. Data Protection Training. [Á neti] The Irish Computer Society, 2010. [Tilgreint: 10. maí 2010.] http://www.ics.ie/index.php/Data-Protection-Training/data-protection-training.html.
11. Valgerður, Gunnarsdóttir. MSc. MPH sérfræðingur. Tölvupóstur. Heilbrigðisráðuneytið, Reykjavík, 31. maí 2010.


Adolf Þór Lúðvíksson, tæknifræðingur hjá Mílu; Sæmundur E. Þorsteinsson, forstöðumaður tæknihögunar og rannsókna hjá Símanum

Flutningur háhraða gagnamerkja innan heimila

Inngangur

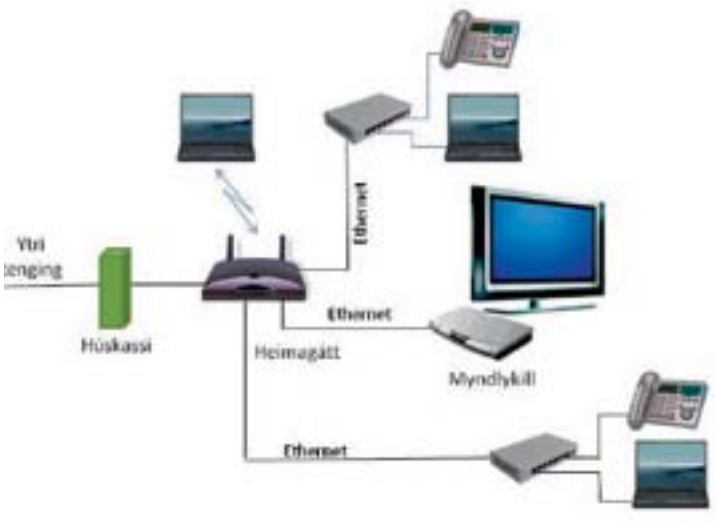
Undanfarin ár hafa heimili átt kost á háhraða gagnafjarskiptum um ADSL-, VDSL- og ljósnet. Framan af var einkum um háhraða internettengingar að ræða en frá árinu 2004 hafa menn átt þess kost að nýta tengingarnar til flutnings sjónvarpsmerkja og er sú þjónusta nú orðin mjög útbreidd. Möguleikar til uppbyggingar heimaneta eru mjög misjafnir. Í gömlum húsum eru oft engar lagnaleiðir fyrir hendi og bæði dýrt og erfitt að koma þeim fyrir. Í sumum nýjum húsum er ástandið hins vegar til fyrirmyndar. Nýlega komu út tæknireglur um fjarskiptalagnir í íbúðarhúsnæði hjá Staðlaráði Íslands [1] en þar er m.a. lagt til að í hverju íverurými verði tveir óháðir fjarskiptatenglar og allar fjarskiptalagnir verði stjörnutengdar til tækjarýmis heimilisins. Þegar háhraða tenging er aðeins nýtt til vefskoðunar, fjarvinnu og fyrir tölvupóst nægir að hafa þráðlaust innanhúss net (WiFi) til að tengja útstöðvarnar og hefur það hentað bærilega um árabil. Streyming sjónvarpsgagna um hefðbundin þráðlaus net hefur hins vegar verið vandkvæðum bundin og hefur þurft að grípa til þráðbundinna lausna. Þar sem fjarskiptalagnir eru ekki fyrir hendi er augljósasta leiðin að leggja netsnúru frá beini til myndlykils en það hefur oft valdið óþægindum á heimilum og þótt til lýta. Til eru fleiri lausnir á þessum vanda sem verða reifaðar í þessari grein. Greinin er byggð á lokaverkefni Adolfs Þórs Lúðvíkssonar sem hann vann sem hluta af námi sínu í tæknifræði við Háskólann í Reykjavík [2]. Verkefnið var unnið hjá Símanum undir stjórn Sæmundar E. Þorsteinssonar og Ólafs Páls Einarssonar.

Gagnaflutningsþarfir innan heimila

Nú er algengt að fólk hafi um 10 – 20 Mb/s tengihraða heim til sín og sumir jafnvel allt að 100 Mb/s en mjög er heiglum hent hvernig tengingin nýtist inni á heimilum. Þráðlaus net sem fara eftir WiFi stöðlum þykja mjög hentug innanhúss, helst hefur verið stuðst við staðlana IEEE 802.11b og 802.11g. Sá síðarnefndi hefur verið alls ráðandi undanfarin ár og er sagður hafa 54 Mb/s hraða en algengt er að menn nái um 20 Mb/s tengingu í raunumhverfi. Þetta nægir vel fyrir hefðbundna notkun internetsins og myndi einnig nægja fyrir flutning sjónvarpsmerkja ef ekki kæmu til ýmsar truflanir eins og margleiðahrif (e. Multipath effect). IEEE 802.11g staðallinn hefur takmarkaða getu til að takast á við deyfingu af völdum margleiðahrifa sem er megin ástæða þess að sjónvarpsflutningur truflast svo að ekki er við unandi. Hver rás með hefðbundnu sjónvarpi þarf um 5 Mb/s flutningshraða með MPEG-2 kóðun sem nú er algeng en aðeins um 2 Mb/s með MPEG-4 kóðun sem ryður sér nú til rúms. Háskerpu sjónvarp þarf um 8 Mb/s með MPEG-4 kóðun en hún er ráðandi kóðunaraðferð fyrir háskerpu sjónvarp. Til viðbótar þessu þarf heimanetið að ráða við skráaflutning milli tölva en þá er gott að hafa sem mestan hraða. Kvikmynd í venjulegri upplausn sem kóðuð er með MPEG-4 aðferð er oft um 700 MB að stærð. Það tæki um 5 mínútur að flytja hana um 20 Mb/s hraða tengingu og um eina mínútu yfir 100 Mb/s tengingu. Margir hafa þegar sett upp heimanet sín þannig að þeir geyma gögn miðlægt og sækja þau á útstöðvar, sem geta verið heimatölvur, „flakkarar“, leikjatölvur nýttar til afspilunar eða myndlyklar. Menn ættu því að hafa það sem markmið að heimanet þeirra nái a.m.k. 50 Mb/s tengihraða.

Leiðir til uppbyggingar heimaneta

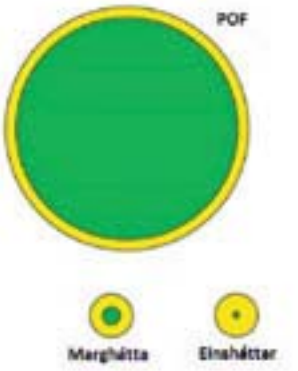
Í þessum kafla verður fjallað um mismunandi leiðir til uppbyggingar heimaneta í húsum þar sem lítt eða ekki hefur verið gert ráð fyrir fjarskiptalögnum á hönnunarstigi. Í [2] voru skoðaðar aðferðir með plastljósleiðurum, fjarskiptum um raflínur og nýjum þráðlausum staðli sem nefndur er IEEE 802.11n. Þessum aðferðum verður lýst nánar en einnig aðferð sem byggist á notkun sjónvarpsdreifikerfa með kóaxstrengjum en slík net eru víða til staðar í íbúðum. Að þráðlausu leiðinni undanskilinni eru þær leiðir sem hér verður lýst almennt til þess að brúa vegalengd milli tveggja punkta innan heimilis. Til dæmis milli beinis (e. router) og myndlykils eða tölvu. Vel er hægt að hafa Ethernet skipti á endunum og líkja þannig eftir stjörnutengdu sambandi frá einum punkti til margra, mynd 1.



Mynd 1. Dæmigert heimanet með IP-sjónvarpi, og Ethernet tengingum.

Plastljósleiðarar

Ljósleiðarar byggja á tækni sem hefur verið til í áratugi. Hefðbundnir ljósleiðarar eru búnir til úr örþunnum þræði sem samanstendur af kjarna úr gleri, klæðningu úr gleri sem umlykur kjarnann og tryggir að ljósgeislinn helst inni í kjarnanum og loks kápu sem ver ljósþráðinn. Hefðbundnir ljósleiðarar henta illa til innanhússtenginga vegna þess að vinna með þá krefst sérþekkingar og –búnaðar, jafnframt er beygjuradíus þeirra takmarkaður og þeir eru viðkvæmir. Plastljósleiðari (e. Plastic Optical Fiber, POF) er oftast búinn til úr ákveðinni tegund af plasti, polymethyl methacrylate (PMMA), þ.e.a.s. hann hefur plastkjarna í stað glers. Kjarninn getur verið 100 sinnum sverari en í hefðbundnum ljósleiðara og er 0,125 – 2 mm að þvermáli, mynd 2. Flutningsgeta flestra POF-kerfa sem nú eru á markaði er 100 Mb/s. Einnig fást kerfi sem hafa 1 Gb/s gagnahraða og jafnvel meiri. Plastljósleiðari með endabúnaði er sýndur á mynd 3. Meðhöndlun plastljósleiðarans er auðveld og á færi flestra og hann þolir mjög lítinn beygjuradíus. Með POF eru skæri eða beittur hnífur einu verkfærin sem þarf til að tengja enda eða stytta ljósleiðarann. Þar sem raf- eða segulsvið hefur engin áhrif á ljósleiðara er hægt að koma POF fyrir nánast hvar sem er í heimahúsum og er m.a. leyfilegt að draga hann í rör ásamt rafmagnsleiðslum. Einnig er hann mjög léttur, sveigjanlegur og sterkur.



Mynd 2. Stærð plastljósleiðara borin saman við marghátta og einhátta ljósleiðara.

Mynd 3. Plastljósleiðarakerfi fyrir tengingu mill tveggja punkta með Ethernet endabúnaði

Fjarskipti um rafstrengi

Fjarskipti um rafstrengi (e. Power Line Communication, PLC) er tækni til þess að flytja gögn um rafmagnslagnir. Fjarskipti um rafstrengi voru upphafleg hugsuð til þess að veita fólki gagnatengingar til heimila og átti m.a. að keppa við ADSL. Í ljós kom að þessi tækni hentaði ekki til fjarskipta yfir langa rafstrengi og því hefur notkunarsvið hennar einkum verið innanhúss. Með þessari tækni þarf engar nýjar eða sérstakar lagnir til að koma á tengingu t.d. milli tölva því rafmagnslagnirnar sem eru til staðar eru nýttar fyrir gagnasamskipti. Nýjasti PLC-búnaðurinn sem nú er á markaði byggir á HomePlug AV (HPAV) staðli, en hann tók við af gamla HomePlug 1.0 (HP1.0) staðlinum sem var gefinn út árið 2000. Þessi búnaður er sagður hafa flutningsgetu upp á 200 Mb/s. HomePlug 1.0 var fyrst og fremst hugsaður til internettenginga en HomePlug AV fyrir flutning á hljóði, mynd og gögnum innan húsveggja.

Nú er komin nokkur reynsla á notkun PLC til innanhússtenginga. Hún er misjöfn, náðst hefur tengihraði um 70 Mb/s en áreiðanleiki sambandsins er stundum ekki nægur til að það henti til flutngings IP-sjónvarps innahúss. PLC hentar þó oftast ágætlega til internettenginga.

WiFi með IEEE 802.11n staðli

WiFi hefur verið notað um árabil og er nú mest stuðst við staðalinn sem heitir IEEE 802.11g. Hann er sagður gefa 54 Mb/s tengihraða en sjaldan ná notendur hraðara sambandi en um 20 Mb/s. Það nægði vel til flutnings IP-sjónvarps ef sambandið væri ekki mjög óstöðugt, það er t.d. háð því að fólk gengur um íbúðina eða hvort dyr standa opnar eða lokaðar. Þetta leiðir til margleiðahrifa sem draga mjög úr gæðum sambandsins. Þetta skiptir ekki máli við venjulegar internettengingar en öllu máli við flutning sjónvarps. IEEE 802.11n staðallinn kom út árið 2009 og boðar byltingu í afkastagetu og áreiðanleika WiFi-neta. Helsta nýjungin er notkun MIMO-tækninnar (Multiple Input Multiple Output) sem þýðir að mörg sendi- og viðtökuloftnet eru notuð til að byggja upp eitt samband. Í heimabúnaði er algengast að hvert tæki hafi tvö loftnet, mynd 4. Segja má að með MIMO séu margleiðahrifin nýtt til að auka gagnahraða en án MIMO eru þau oftast til vandræða. Til að minnka áhrifin af völdum margleiðahrifa notast MIMO við rúmfléttun (e. Spatial Multiplexing). MIMO búnaður sendir út marga gagnastrauma sem ferðast eftir mörgum leiðum frá sendi til móttakara. Hver merkjastraumur er sendur frá sér loftneti sem notar sinn sendi, alltaf er bil á milli loftneta þannig að hvert merki fer sína eigin leið, kallast þetta rúmmargbreytni (e. Spatial Diversity). Þegar merkið kemur til móttakara er hver straumur afkóðaður, öll merkin frá hverjum straumi eru svo sameinuð og samanlögð útkoma skilar betra merki en hægt er að ná fram með einu loftneti.

Mynd 4. MIMO búnaður ætlaður til notkunar á heimilum.

Auk MIMO er kostur á tvöfaldri bandbreidd í IEEE 802.11n, þ.e. hægt er að nota rásir sem eru 40 MHz breiðar í stað 20 MHz rása sem notaðar eru í IEEE 802.11g. Með eftirtöldum aðgerðum verður niðurstaðan sú að með IEEE 802.11n getur náðst 600 Mb/s gagnahraði eða rífleg tífföldun umfram 802.11g.

- Fleiri undirburðarbylgjur (e. Subcarriers), úr 48 í 52 sem eykur hraðann úr 54 Mb/s í 58,5 Mb/s.
- Aukinn FEC (e. Forward Error Correction) kóðunarhraði úr 3/4 í 5/6 sem eykur hraðann í 65 Mb/s.
- Svonefnt varnarbil er minnkað úr 800 ns í 400 ns sem eykur hraðann í 72,2 Mb/s.
- MIMO tæknin gerir kleift að nota fjóra aðskilda gagnastrauma sem eykur gagnahraðann í 288,9 Mb/s.
- Aukin bandbreidd, búin er til 40 MHz rás úr tveimur 20 MHz rásum og fjölgar það undirburðarbylgjum í 108 og eykur hraðann í 600 Mb/s.

Prófað var að nýta IEEE 802.11n til háskerpu IP-sjónvarpsflutnings í steinsteyptu húsi á þremur hæðum. Engar truflanir komu fram fyrr en sendir var staðsettur á neðstu hæð og móttakari á efstu hæð, við þær aðstæður þurfti merkið að fara í gegnum tvær steinsteyptar gólfplötur. Hins vegar virkaði allt mjög vel þegar sendirinn var staðsettur á miðhæð og

Margir hafa þegar sett upp heimanet sín þannig að þeir geyma gögn miðlægt og sækja þau á útstöðvar, sem geta verið heimatölvur, „flakkarar“, leikjatölvur nýttar til afspilunar eða myndlyklar.

Ljósleiðarar byggja á tækni sem hefur verið til í áratugi.

Fjarskipti um rafstrengi voru upphaflega hugsuð til þess að veita fólki gagnatengingar til heimila og átti m.a. að keppa við ADSL.

Kóax-strengir eru mun betri flutningsmiðill en símalínur og því næst mjög góður árangur með nýtingu þeirra.

móttakarinn var staðsettur annað hvort á jarðhæðinni eða á 3.hæð. Engar truflanir komu fram á sjónvarpinu hvort sem dyr voru lokaðar eða opnar og umgangur í kringum móttakarann.

802.11n búnaðurinn sem var notaður getur flutt háskerpu sjónvarpsmerki án vandræða við þær aðstæður sem búnaðurinn var prófaður í. Búnaðurinn ræður einnig við að senda 2 háskerpu strauma á tvo myndlykla samtímis. Ekki komu fram truflanir þótt bilið milli sendis og móttakara væri um 15 metrar með gips- og glerveggjum á leiðinni. Á það skal bent að þráðlaus sambönd geta ávallt orðið fyrir truflunum og eru því ekki eins áreiðanleg og sambönd um ljósleiðara eða koparþræði.

Notkun sjónvarpsdreifikerfa

Hægt er að nota innanhúss sjónvarpsdreifikerfi sem byggð eru á kóax-strengjum til uppbyggingar á heimanetum. Þetta hefur ekki áhrif á sjónvarpsflutninginn sjálfan, notast er við tíðnisvið utan sjónvarpstíðnisviða. Þessi búnaður byggist á stöðlum frá Home Phone Networking Alliance [5] sem voru upphaflega samdir til að nýta símalínur fyrir háhraða gagnaflutning. Kóax-strengir eru mun betri flutningsmiðill en símalínur og því næst mjög góður árangur með nýtingu þeirra. Kóaxstrengirnir hafa það einnig umfram rafmagnsstrengi að vera lausir við truflanir. Nú bjóðast kerfi sem sögð eru geta flutt 200 Mb/s. Við mælingar hefur náðst rúmlega 60 Mb/s hraði sem dugir vel til flutnings margra háskerpu IP-sjónvarpsrása ásamt internettengingum. Hægt er að fá búnaðinn í mjög svipuðu formi og búnað til rafstrengjafjarskipta, þ.e. honum er stungið beint í 230 V tengil og kóax- og Ethernet-strengir tengdir við hann.

Lokaorð

Hér hafa verið bornir saman nokkrir kostir sem fyrir hendi eru til uppbyggingar háhraða heimaneta, m.a. til flutnings háskerpu IP-sjónvarps. Vel má nota mismunandi lausnir í sama heimanetinu og velja þær með tilliti til kostnaðar og getu. Þannig getur plastljósleiðari hentað mjög vel til að koma merkjum milli hæða í húsum en þráðlaus lausn með IEEE 802.11n til að dreifa merkjum innan rýma. Í töflu 1 er að finna samanburðaryfirlit á þeim lausnum sem hér voru kynntar og þá einkunn sem höfundar hafa gefið einstökum lausnum.

Tafla 1. Samanburður lausna til uppbyggingar háhraða heimaneta

	802.11n	POF	PLC	kóax hPNA
Tenging	Þráðlaust	Þráður	Þráður	Þráður
Áreiðanleiki	+	++	++	++
Þægindi við uppsetningu	+	-	++	+
Þörf á tæknilausnum	Já	Já	Nei	Varla
Öryggi	++	++	++	++
Raunhraði	90 Mb/s *	100 Mb/s	70Mb/s *	60 Mb/s

**Við bestu aðstæður, - = Ekki gott, + = Gott, ++ = Mjög gott*

Heimildir

[1] „Tækinreglur um fjarskiptalagnir í íbúðarhúsnæði“, Staðlaráð Ísland, 2008.
[2] Adolf Þór Lúðvíksson, „Hermun DSL sambanda og flutningur IP sjónvarps“, lokaverkefni í tæknifræði, Háskólinn í Reykjavík, 2009.
[3] HomePlug Alliance, HomePlug AV white paper. http://www.homeplug.org/tech/whitepapers/HPAV-White-Paper_050818.pdf, 2005
[4] http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/prod_white_paper0900aecd806b8ce7_ns767_Networking_Solutions_White_Paper.html
[5] http://www.homepna.org/

**Ólafur Andri Ragnarsson,
hugbúnaðararkítekt hjá Betware og
aðjúnkt við Háskólann í Reykjavík**

Auðvitað er iPad ekkert annað en tölva undir glansandi viðmóti. Og auðvitað er þarna um að ræða alvöru stýrikerfi sem keyrir vélina áfram. En það sem er mikilvægt við iPad, líkt og frændann iPhone, er að þetta er falið.

iPad áhrifin

Tæknifréttir fyrir og um síðustu páska snerust nánast aðeins um eitt, nýju iPad tölvuna frá Apple. Þó svo að þetta hafi ekki verið fyrsta töflutölvan fékk hún ótrúlega mikla umfjöllun í fjölmiðlum og löngu áður en tölvan var gerð opinber voru margir búnir að segja skoðun sína á henni. iPad fylgir í fótsport frænda síns, iPhone sem hafði gríðarleg áhrif á símamarkaðinn. Ef við berum iPad saman við iPhone þá má velta fyrir sér hvaða áhrif iPad muni hafa á tölvumarkaðinn og hvernig fólk notar tölvur. Hver verða eiginlega iPad áhrifin?

Er iPad tölva?

Til að átta sig á iPad þá er fyrst að nefna að iPad er fyrst og fremst neytendatæki frekar en hefðbundin tölva. Það er nokkur munur á tölvum og neytendatækjum. Tölvur hafa hingað til verið mjög tæknilegar og það krafist nokkurrar þekkingar að nota þær. Þeir sem hafa sett upp internet tengingu í gegnum tíðina þekkja það. Þar fyrir utan eru endalausir valkostir, oft frekar tæknilegir, settir í hendur notenda sem hafa engan áhuga á slíkum kostum. Hverjum er ekki sama hvort notaður sé MIME staðallinn þegar viðhengi er sent í tölvupósti? Auðvitað er iPad ekkert annað en tölva undir glansandi viðmóti. Og auðvitað er þarna um að ræða alvöru stýrikerfi sem keyrir vélina áfram. En það sem er mikilvægt við iPad, líkt og frændann iPhone, er að þetta er falið.

Við þurfum reyndar ekki að fara langt til að finna tölvu sem er dulbúin sem neytendatæki. PlayStation 3 er dæmigert neytendatæki. Mjög öflug tölva en afar einföld í notkun. PS3 hefur tvo hnappa. Annar er til að kveikja og slökkva og hinn til að opna hólfið sem tekur diskana. Stýrikerfið er einföld valmynd með áherslu á að spila afþreyingarefnið sem sett er í vélina, hvort sem það er nýjasti tölvuleikurinn eða Blu-Ray mynd. Hver sem er getur notað vélina án nokkurrar fyrirhafnar. Á mörgum heimilum er þetta öflugasta tölvan í húsinu og jafnframt sú auðveldasta í notkun.

Hver þarf möppur og skjalaskáp?

Það sem er áhugavert við iPad er viðmótið á stýrikerfinu. Síðan á 8. áratugnum hefur skrifstofusamlíkingin (e. desktop metaphore) ráðið í viðmóti. Það réðst af því að markhópurinn fyrir tölvur voru fyrst og fremst fyrirtæki þ.e. skrifstofur. Skrám er raðað í möppur, þær opnaðar og lokaðar, vistaðar og flokkaðar. Öllum er einnig ljóst að unnið er á diski tölvunnar.

Í dag eru notendur venjulegt fólk, neytendur. Fólk sem vinnur ekki endilega á skrifstofu. Fólk sem hefur engan sérstakan áhuga á að læra á þá tækni sem býr að baki. Það er að skoða vefinn, horfa á myndskeið, hlusta á tónlist, spila tölvuleiki, fylgjast með vinum sínum á Facebook og MySpace og lesa fréttir og blogg. Þessi notkun er langt frá því að vera eitthvað í líkingu við skrifstofu. Það er ljóst að iPad er að brjótast undan samlíkingunni við skrifstofuna og leggur áherslu á vefinn og það að njóta afþreyingarefnis eins og tónlistar, þátta og kvikmynda.

Músartegund í útrýmingarhættu

Annað áhugavert við iPad er að músin er fjarri. Músin var fyrst kynnt 1968 og kom fyrir sjónir almennings í byrjun 9. áratugarins með Lisu Apple og skömmu síðar Macintosh. Músin hefur reynst vel en sem inntakstæki er hún er ófullkomin og alls ekki eins náttúruleg og það að nota puttann. Fjöldi dæma sýna að börn á leikskólaaldri geta tileinkað sér iPad án nokkurrar tilsagnar.

Þess má líka geta að töflutölvur eru alls ekki nýjung. Microsoft kom með Tablet PC árið 2002. Sú tölva náði ekki að taka flugið. Ástæðan er líklega sú að fólk leit á slíkar tölvur einmitt sem tölvur. Viðmót var að mestu svipað og á venjulegum tölvum nema að það vantaði lyklaborðið og músina. Því var Tablet PC eins og léleg útgáfa af hefðbundinni tölvu. iPad getur náð að forðast þessa gildru þar sem allt viðmót er ekki nákvæmlega eins og venjuleg tölva. Snertiskjárinn í iPad er lykillinn að þessu.

Hvort iPad á eftir að breyta tölvusögunni er of snemmt að segja. Þó gefa sölutölur sterkar vísbendingar um að þarna hafi opnast nýr markaður. iPad er vélin sem hægt er að hafa í eldhúsinu, taka með sér á klósettið í stað dagblaðsins og hægt er að nota til að lesa í rúminu. Fyrstu viðbrögð við iPad voru mjög ólík – annað hvort fannst mönnum þetta frábært tæki eða vélinni var spáð niðurlægjandi dauðdaga. Ef við skoðum söguna þá hefur tækni sem hefur haft áhrif á söguna einmitt fengið slík viðbrögð. Þegar PC vélin kom fyrst fram voru tölvuframleiðendur og notendur stórra véla fljótir að afgreiða hana sem afkastalítið leiktæki. En þeir sem ekki voru í þessum hópi og höfðu almennt ekki aðgang að tölvum, tóku henni opnum örmum. Ef fyrstu vikur iPad eru til vitnis um eitthvað þá erum við núna að hefja áratug töflutölvunnar.

Eyður skrifar:

Öryggi er ekki vara sem hægt er að bæta inn eftirá, heldur hugarfar.

Traustustu kerfi geta ekki varist aðstoðarlaust nema í stuttan tíma.

Hver gætir varðmannanna?

Ég vann eitt sinn fyrir vestan hjá hugbúnaðarfyrirtæki sem var umhugað að söluvaran væri í lagi. Starfsmenn prófunardeildar voru metnaðargjarnir enda voru einkunnarorðin: „við afhendum engin forrit fyrr en þau eru tilbúin“. Forritararnir gerðu góðlátlegt grín að þessu með einkunnarorðunum: „afhendum allt sem sleppur gegnum þýðandann“ - En þeir meintu það ekki.

Á hverri nóttu voru þúsundir prófana keyrðar á nýþýddum kóða. Sá sem átti kóða sem stóðst ekki próf var kallaður inn á kontór. Ef einhver sendi inn kóða sem þýddist ekki og olli því að ekki var hægt að keyra neinar prófanir um nóttina var sá hinn sami sendur til forstjóra og var í verulega slæmum málum; allir vissu þegar það hafði gerst.

Allir notuðu sama gamla C þýðandann, sem var viljandi hafður nokkurra ára gamall vegna þess að allir höfðu fengið tíma til að kynnast honum og vissu hvernig hann hegðaði sér. Ég var hneykslaður á að fyrirtækið var ekki komið með C++ en sá seinna spekina í þessu. Viðskiptavinirnir vildu gæði og öryggi og voru tilbúnir að borga fyrir, þetta var „þannig bransi“. Tilbúnir rammar og forritasöfn voru ekki vinsæl, þau voru „ekki okkar uppfinning“.

Öryggi er ekki vara sem hægt er að bæta inn eftirá, heldur hugarfar sem kaupandi og seljandi verða að tileinka sér frá byrjun. Það er ekki hægt að taka verslunarmiðstöð og gera á henni smávægilegar breytingar til að breyta henni í fangelsi. Til þess eru glerþökin og útgangarnir of margir. Þeir sem hafa rætt um að láta útrásarvíkingana afplána í einni slíkri ættu að hugsa sig um.

Flest tæknileg vandamál tengd öryggismálum eru vel þekkt og leyst. Við kunnum að dulkóða skilaboð þannig að enginn óboðinn getur lesið þau, þótt öðru sé haldið fram í bíómyndum, þar sem tölvunördinn brýst inn á nokkrum mínútum. Það er hægt að undirrita skjöl með rafrænum hætti og gefa út rafræn skilríki.

Flest óleystu vandamálin eru mannleg. Ég þekki engan sem dulkóðar eða undirritar tölvupóst, þótt forritið PGP sé ókeypis og þægilegt í notkun. Lykilorð eru illa valin og illa varin - oft eru þau skrifuð á miða undir músamottunni. Kevin Mitchnick sem sat inni fyrir innbrot í tölvukerfi sagðist ekki hafa beitt tæknibrellum við innbrotin heldur þóttist hann vera starfsmaður tölvudeildar og spurði starfsfólk hvert lykilorðið væri, með góðum árangri.

Það er ekki nóg að byggja traust kerfi ef notendur ætla ekki að vera hluti í öryggisferlinu. Jafnvel sterkustu lásar verða brotnir upp á endanum, ef sá sem reynir að brjóta þá er staðfastur, hefur tíma og næði til að vinna án þess að vera uppgötvaður. Fyrirtæki gefa þjófum of oft næði til að vinna vinnuna sína. Oft sýna dagbækur í tölvukerfum merki um tilraunir til innbrota löngu áður en þau heppnuðust, en dagbækurnar voru bara ekki skoðaðar fyrr en um seinan. Traustustu kerfi geta ekki varist aðstoðarlaust nema í stuttan tíma. Þegar ég gerði mér grein fyrir þessu fór ég að læsa hjólinu mínu á fjölförnum stöðum, þar sem þjófurinn gæti ekki dýrkað lásinn upp í friði.

Mörgum reynist erfitt að meta áhættur og hvar peningum er best varið til að minnka þær. Ég heyrði um mann sem byrjaði hvern dag á bjór og línu af kóki í nös en fékk sér svo Diet Pepsi af því hann var að reyna að lifa heilbrigðu lífi. Margir álíta að sporðdrekar séu hættulegir en samt deyr bara einn Bandaríkjamaður á ári úr sporðdrekastungu meðan 43 þúsund þeirra deyja í bílslysi.

Þannig held ég að tölvuöryggismál margra séu byggð á óraunsæju áhættumati. Peningum er varið í vírusvarnir, á sama tíma og harðir diskar eru ekki afritaðir, eða fartölvur eru skildar eftir á glámbekk. Hversu oft hefur ekki birst frétt um að viðkvæm gögn frá Scotland Yard hafi tapast á ferðatölvu, eða um doktorsritgerðina sem glataðist þegar tölvan gleymdist í strætó?

Öryggismál tölva má skilgreina í víðu samhengi. Ég gæti rökstutt að tölvur eigi stóran þátt í hruninu á Íslandi og að öryggismálin þar hafi ekki verið í lagi því þær leyfðu fjármálagerninga sem fæstir ef nokkrir gátu skilið. Það er mannlegt að gera mistök, en til að klúðra hlutunum algjörlega þarf tölvu.

Oft eru menn í lykilstöðum veikasti hlekkurinn í öryggismálum fyrirtækja. Þeir eru með öflugustu lykilorðin og geta gert mestan skaða, viljandi og óviljandi. Sókrates spurði: „Hver gætir varðmannana“ og varð fátt um svör. Þeir sem bera ábyrgð á tölvumálum verða iðulega að bera ábyrgð á sjálfum sér, vera menn sem aðrir geta treyst. Hvað ef þeir eru það ekki en haga sér eins og útrásarvíkingarnir gerðu?

Ég heyri sjaldan um skaðabótamál gegn fyrirtækjum sem voru ekki með öryggið í lagi. Sennilega er það hluti af skýringunni hvers vegna öryggismál eru ekki í lagi. Ef galli í hugbúnaði kostar framleiðandann ekkert hver er þá hvatningin til að fækka þeim?

Friðrik Skúlason fær Upplýsingatækniverðlaun Skýrslutæknifélags Íslands

Fimmtudaginn 20. maí afhenti Gylfi Magnússon, viðskiptaráðherra, heiðursverðlaun Skýrslutæknifélags Íslands en verðlaunin eru nú veitt í fyrsta sinn. Þau eru veitt til einstaklings fyrir framúrskarandi framlag til upplýsingatækni á Íslandi. Afhending verðlaunanna var hluti af dagskrá UT dagsins sem fram fór í Salnum í Kópavogi. Verðlaunin eru veglegur verðlaunagripur, hannaður af listakonunni Ingu Elínu, ásamt heiðursskjali.

Valið fór þannig fram að félagsmönnum í Skýrslutæknifélaginu var boðið að tilnefna einstakling eða forsvarsmann fyrirtækis sem hefur skarað framúr á sviði upplýsingatækni, skapað verðmæti og auðgað líf Íslendinga með hagnýtingu á upplýsingatækni. Það var í höndum valnefndar sem skipuð er af stjórn Skýrslutæknifélagsins að velja heiðursverðlaunahafann fyrir árið 2010. Nefndin lagði áherslu á það í störfum sínum að framlag viðkomandi hefði sannað sig með afgerandi hætti.

Í mati valnefndar kemur fram að Friðrik er einn fyrsti Íslendingurinn til að átta sig á möguleikum netviðskipta og sölu sérhæfðs hugbúnaðar yfir netið. Þannig tókst honum fljótt að gera allan heiminn að markaðssvæði fyrir vöru sína. Þetta gerði hann löngu áður en flestir Íslendingar höfðu gert sér grein fyrir notkunarmöguleikum netsins eða vissu yfirhöfuð af tilvist þess. Hugbúnaður sem hann hefur komið að hefur verið hagnýttur af mörgum tölvunotendum hér heima og erlendis.

Forritið sem kom Friðriki á kortið var fyrst gefið út árið 1989 og heitir Lykla Pétur. Það má ætla að ein milljón tölvunotenda út um allan heim noti hugbúnað sem hann hefur unnið að. Hjá fyrirtæki hans, Friðrik Skúlason ehf., starfa nú um 50 manns.

Veiruvarnarforritið Lykla Pétur, eða F-Prot Antivirus, eins og það heitir á ensku, hefur aukið tölvuöryggi hjá fjölda notenda. Friðrik hefur verið óþreytandi við að fjalla um tölvuöryggismál í ræðu og riti þannig að eftir hefur verið tekið. Samskipti, viðskipti og stjórnsýsla fara í vaxandi mæli fram á netinu og því fylgir aukið mikilvægi öryggismála. Erindi hugbúnaðarins sem Friðrik hefur byggt fyrirtæki sitt á er því áfram brýnt þó langt sé um liðið síðan fyrsta útgáfa hans kom á markaðinn.

Ættfræðiáhugi Íslendinga stendur á gömlum grunni. Með því að koma ættfræðiupplýsingum úr margvíslegum bókum og blöðum yfir á aðgengilegt og stafrænt form Íslendingabókar á netinu hefur Friðrik Skúlason í samstarfi við Íslenska erfðagreiningu fengið marga Íslendinga til að tileinka sér netnotkun. Markhópurinn var mjög stór því margir Íslendingar hafa áhuga á ættfræði. Hluti þess hóps hefði trúlega ekki stigið fæti inn í netheima ef Íslendingabók hefði ekki komið til sögunnar og veitt þeim áður óþekkta sýn á ættfræðiupplýsingar. Í þessu verkefni nýttu Friðrik og hans samstarfsmenn ættfræðiforritið Espólín sem Friðrik vann að á sínum tíma.

Þar að auki hefur fyrirtæki Friðriks sett á markað ritvilluvörn sem ber heitið Púki og hefur hann nýst mörgum vel í leik, námi og störfum.

Valnefndin í ár samanstóð af Guðbjörgu Sigurðardóttur og Sigurjóni Péturssyni, heiðursfélögum Ský, Þórólfi Árnasyni, formanni samtaka upplýsingatæknifyrirtækja, Ebbu Þóru Hvannberg frá HÍ ásamt Eggert Claessen hjá Frumtaki. Með nefndinni störfuðu Jón Heiðar Þorsteinsson, úr stjórn Skýrslutæknifélagsins, og Arnheiður Guðmundsdóttir, framkvæmdastjóri félagsins.

Heiðursfélagar fallnir frá

Óttar Kjartansson
f. 7. ágúst 1930
d. 17. apríl 2010

Fyrsta íslenska fyrirtækið á því sviði atvinnulífsins sem nú nefnist upplýsingatækni var stofnað árið 1952. Heiti þess var upphaflega Skýrsluvélar ríkisins og Reykjavíkurbæjar, en síðar varð skammstöfunin Skýrr að heiti þess og vörumerki. Stofnendur voru Hagstofa Íslands f.h. Ríkisstjórnarinnar og Rafmagnsveita Reykjavíkur f.h. Reykjavíkurbæjar. Skýrsluvélar tóku við rekstri gagnavinnsluvéla sem Hagstofan hafði nýlega aflað sér ásamt samningi er Rafmagnsveitan hafði gert við IBM um leigu á vélasamstæðu. Fyrstu starfsmenn Skýrr komu frá Rafmagnsveitunni og Hagstofunni. Óttar Kjartansson kom til Skýrsluvéla frá Rafmagnsveitu Reykjavíkur þar sem hann hafi unnið frá 1948. Ekki var langt að fara því hið nýja fyrirtæki fékk inni í einu herbergi hjá Rafmagnsveitunni í Tjarnargötu 12. Óttar starfaði hjá Skýrr í fimmtíu ár. Fjórum síðustu starfsárunum varði hann í að taka saman sögu fyrirtækisins. Kom hún út á bók árið 2002: Upplýsingaiðnaður í hálfa öld. Saga Skýrr 1952-2002, 350 blaðsíðna verk, ómetanleg heimild um upphaf vélrænnar gagnavinnslu á Íslandi.

Óttar Kjartansson lést 17. apríl árið 2010 á líknardeild Landspítala háskólasjúkrahúss, rétt tæplega áttræður að aldri, fæddur 7. ágúst 1930. Hann ólst upp í Reykjavík, átti í æsku heima í Lækjargötunni, en dvaldi hjá ættingjum úti á landi á sumrin. Hann kvæntist árið 1965 Jóhönnu Stefánsdóttur hjúkrunarfræðingi. Börn þeirra eru Oddný Kristín fædd 1968 og Kjartan Sævar fæddur 1974. Fyrsta barn þeirra, Stefán, fæddur 1967, dó aðeins fjögurra daga gamall.

Óttar átti farsæla vegferð. Hann lauk ekki langskólanámi en eðlisgreind hans var slík að hann gat tileinkað sér vandasöm verkefni og leyst þau með prýði á sviði sem ætla mætti að farsælla væri að byggja á langskólanámi. Hann var meðal fyrstu sérmenntuðu kerfisfræðinga hér á landi, lærði þau fræði hjá IBM í Danmörku, og átti þátt í skipulagningu og forritun fjölda verkefna í áranna rás. Hæfni hans á þessu sviði var óvefengjanleg og störf hans farsæl. Hann fór sjaldan mikinn og barst ekki á á tímum sviptinga og breytinga heldur vann störf sín af alúð og kostgæfni. Hann var enda hvers manns hugljúfi og vinsæll jafnt í starfi sem einkalífi. Tryggð við sama vinnuveitanda lýsir mannkostum hans á tímum er margir töldu það sér til gildis að hafa starfað sem víðast.

Óttar var félagslyndur maður og vinafastur. Til hans var jafnan gott að leita. Hann var hjálpsamur og áhugasamur um annarra hag. Leitun var að prúðari manni í framkomu og háttvísi hans var við brugðið. Jafnvel tölvupóstar frá honum bera þessum eiginleika hans vitni. Eigi að síður gat hann verið skoðanafastur en þó með hinni mestu hófsemd.

Óttar var gerður að heiðursfélaga Skýrslutæknifélags Íslands á aðalfundi 29. janúar 2004. Hann var fyrsti starfsmaður félagsins og aðstoðarmaður fyrsta formannsins, Hjörleifs Hjörleifssonar, 1968-1975. Þegar hafin var útgáfa tímaritsins Tölvumála árið 1976 varð hann formaður ritnefndar, ritstjóri og ábyrðarmaður. Gegndi hann því ábyrgðarstarfi allt til 1982. Þá var hann ritari Skýrslutæknifélagsins frá 1975 til 1981.

Þegar nokkrir frumherjar undir forystu Odds Benediktssonar tóku sér fyrir hendur árið 2003 að setja saman erindi til flutnings á ráðstefnu um sögu upplýsingatækninnar á Norðurlöndum var Óttar að sjálfsögðu til kallaður og átti drjúgan hlut í því sem Oddur fór með til Þrándheims. Upp úr þessu starfi var stofnuð árið 2004 Öldungadeild Skýrslutæknifélagsins, sem er faghópur um sögu upplýsingatækninnar á Íslandi. Óttar var meðal stofnenda Öldungadeildarinnar og sat í stjórn hennar fyrstu fjögur árin. Hann samdi einnig erindi til flutnings á næstu ráðstefnu um sama efni er haldin var í Finnlandi árið 2007. Óttar átti ekki heimangengt, en Jóhann Gunnarsson flutti erindið í hans nafni. Er það birt í útgefnu erindasafni frá ráðstefnunni.

Óttar átti ýmis áhugamál sem hann sinnti af sömu kostgæfni og ævistarfinu. Hann var góður ljósmyndari, ferðaðist víða og þekkti landið afar vel. Þá áttu þau hjón nokkra hesta og voru virkir félagar í hestamannafélaginu Gusti í Kópavogi. Óttar sá í mörg ár um útgáfu fréttabréfs fyrir það félag og var meðal ritstjóra afmælisbókar Gusts er út var gefin árið 2000.

Það verður tæplega á nokkurn mann hallað, þótt Óttari sé skipað í hóp frumkvöðla tölvutækninnar á Íslandi. Þekking hans og reynsla á því sviði var margvísleg og óvenjuleg. Hans verður þó ekki síður minnst fyrir prúðmennsku sína og hæversku. Hann var drengur góður og stilltur vel. Geta væntanlega allir tekið undir það, sem til hans þekktu.

Megi minning hans lifa.
Jóhann Gunnarsson, Sverrir Ólafsson

Oddur Benediktsson
prófessor
f. 5. júní 1937
d. 17. ágúst 2010

Tölvur, sem í fyrstu voru kallaðar rafeindareiknivélar eða rafreiknar, tóku að ryðja sér til rúms við háskóla og rannsóknarmiðstöðvar erlendis um miðja tuttugustu öldina. Hinar fyrstu þeirra voru hannaðar og smíðaðar í einu eða afar fáum eintökum og oft með tiltekna notkun í huga. Fyrstu tölvurnar sem framleiddar voru í umtalsverðu magni og ætlaðar til sölu á markaði voru frá fyrirtækinu IBM. Þetta voru IBM 1401 og IBM 1620, settar á markað 1959.

Upp úr 1960 komu til starfa á Íslandi nokkrir vísindamenn sem kynnst höfðu rafreiknum við nám og störf erlendis. Oddur Benediktsson var einn þeirra, hafði numið vélaverkfræði og hagnýta stærðfræði í Bandaríkjunum. Í tengslum við námið hafði hann unnið við rafreikni af gerðinni IBM 650 og komist í kynni við forritunarmálið Fortran.

Um þessar mundir var í undirbúningi að setja á fót Raunvísindastofnun Háskólans og var í því samhengi meðal annars rætt um kaup eða leigu á rafreikni fyrir skólann. Lyktaði því máli svo að Framkvæmdabanki Íslands, sem hélt þá upp á 10 ára afmæli, gaf skólanum fé til að kaupa rafreikni af gerðinni IBM 1620 model II. Ný háskólastofnun, Reiknistofnun Háskóla Íslands, var stofnuð um rekstur vélarinnar og henni fengið húsnæði í kjallara Raunvísindastofnunar við Dunhaga. Magnús Magnússon var ráðinn forstöðumaður Reiknistofnunar og Oddur Benediktsson, sem hafði aðstoðað hann við að undirbúa komu vélarinnar, varð fyrsti starfsmaður hennar. Þetta gerðist síðari hluta árs 1964, en rafreiknirinn mun hafa unnið sitt fyrsta verk á Þorláksmessu það ár.

Allt frá þeim tíma varð Oddur áhrifamaður í þróun og framgangi upplýsingatækni á Íslandi. Hann átti glæsilegan námsferil, lauk stúdentsprófi frá MR árið 1956 og hélt til frekara náms við Rensselaer Polytechnic Institute í New York. Hann lauk BME-gráðu í vélaverkfræði og stærðfræði árið 1960, M.S. í stærðfræði 1961 og Ph.D. í hagnýtri stærðfræði 1965.

Þegar litið er yfir starfsferil Odds við ævilok er ljóst að markviss vinnubrögð hans, glögg dómgreind á það hvað skipti máli og sú gáfa, er honum var gefin í ríkum mæli, að miðla víðtækri þekkingu sinni og hvetja aðra til góðra verka, hafa skilað þjóðinni miklum verðmætum. Af störfum hans fer mest fyrir kennslunni, en á því tímabili sem hann var sérfræðingur við Reiknistofnun kenndi hann miklum fjölda fólks, innan og utan Háskóla Íslands, forritunarmál, í fyrstu aðallega Fortran, sem var nýjung hér á landi og mikil bylting samanborið við að forrita á vélamáli eða Assembler.

Árið 1973 hóf Oddur störf sem dósent við stærðfræðiskor HÍ, en fluttist yfir í tölvunarfræðiskor þegar hún var stofnuð. Hann var einn af aðalskipuleggjendum námsbrautar í tölvunarfræðum við HÍ, var meðal annars formaður nefndar sem samdi námskrána í því fagi og síðar formaður nefndar sem skipulagði námskrá í hugbúnaðarverkfræði. Árin 1982–2007 gegndi Oddur prófessorsstöðu við tölvunarfræðiskor. Hann sinnti ýmsum stjórnunarstörfum fyrir Háskólann, var skorarformaður í tölvunarfræði í mörg ár og í stjórn Reiknistofnunar í um 20 ár. Hann var varaforseti raunvísindadeildar HÍ 1995 til 1997. Rannsóknir Odds beindust meðal annars að upplýsingakerfum og gæðastjórnun í hugbúnaðargerð.

Utan Háskóla Íslands voru helstu störf Odds þessi: Hann starfaði við fjarskiptakerfi gervitungla hjá Bell Laboratories 1962-63, hjá IBM á Íslandi og sat í stjórn félagsins 1969-72. Hann var yfirmaður tæknideildar Skýrr 1972-73 jafnframt stundakennslu við HÍ. Í leyfi frá HÍ árið 1997 starfaði hann við gæðastjórnun hugbúnaðarframleiðslu hjá EJS hf. Þá stofnaði hann árið 1985 fyrirtækið Tölvuþekkingu og átti það í fjögur ár. Oddur kom víða við í ráðgjafarstörfum, meðal annars fyrir Reiknistofu bankanna og ráðuneyti sjávarútvegs, menntamála og fjármála. Hann var formaður nefndar á vegum Rannsóknarráðs Íslands er gaf árið 1986 út álitsgerð og tillögur um stefnumótun á sviði upplýsingatækni.

Oddur gerði sér snemma grein fyrir þýðingu staðla enda ljóst að notkun staðla er lykillinn að vönduðum vinnubrögðum því nær á hvaða sviði atvinnulífsins sem er. Hann var hvatamaður að stofnun samtaka um stöðlun í upplýsingatækni, UT-staðlaráðs árið 1988, en áður hafði sami hópur starfað í skamman tíma undir heitinu Tölvuráð. Oddur var formaður UT-staðlaráðs til 1992. Innan vébanda þess tók hann þátt í norrænum staðlasamtökum, INSTA-IT og leiddi það samstarf meðal annars til útgáfu bókar sem hann ritstýrði og samdi að hluta, MSQH (Modelling a software quality handbook). Fór sú bók víða og varð kveikjan að alþjóðlega staðlinum ISO 9000-3. Oddur starfaði í tækninefndum á vegum alþjóðlegra staðlasamtaka, til dæmis ISO og IEEE. Hér heima var hann meðal höfunda að Innkaupahandbók um upplýsingatækni sem fjármálaráðuneytið gaf út í tveimur útgáfum, 1984 og 1988.

Oddur var frumkvöðull á sínu sviði og hlaut fjölmargar viðurkenningar fyrir störf sín. Hann hlaut verðlaun Ásu Wright árið 1996 og var sama ár valinn tölvumaður ársins hjá PC World Ísland. Árið 1993 var Oddur útnefndur heiðursfélagi Skýrslutæknifélags Íslands vegna brautryðjandastarfa í upplýsingatækni og fyrir félagið. Félag tölvunarfræðinga gerði Odd að fyrsta heiðursfélaga sínum árið 1997. Hann hlaut IBM Fellowship 1960-61 og Rickett's Price við útskrift 1960. Auk þess fékk hann alþjóðlegan námsstyrk vegna frammistöðu í námi.

Oddur Benediktsson starfaði alla tíð ötullega á vettvangi Skýrslutæknifélags Íslands. Hann var varaformaður 1976-7 og formaður árin 1977-1979. Mörg erindi hefur hann flutt á fundum félagsins. Hann var tekinn í tölu heiðursfélaga Skýrslutæknifélagsins á tuttugu og fimm ára afmæli þess. Á meðan Oddur var í stjórn hóf fagtímarit Skýrslutæknifélagsins, Tölvumál göngu sína, og sat Oddur í fyrstu ritnefnd þess. Í formannstíð hans voru ýmis málefni til umræðu, t.d. var ofarlega á baugi að sett yrðu lög um meðferð persónuupplýsinga í tölvum. Fjallað var um mikilvægi tölvunotkunar við stjórn fyrirtækja og um gagnasendingar um símkerfið. Grunnurinn að íslenskri stafagerð í stafatöflum og lyklaborði var lagður og Oddur kom að margvíslegum verkefnum sem stuðluðu að stöðlun í upplýsingatækni.

Í seinni tíð ber mest á frumkvæði hans að stofnun Öldungadeildar SKÝ, faghóps sem vinnur að varðveislu sögulegra minja um upplýsingatæknina. Þegar boðað var til ráðstefnu á vegum IFIP um sögu upplýsingatækninnar á Norðurlöndum kallaði hann saman hóp frumherja til að taka saman erindi um upphaf gagnavinnslu í íslenskri stjórnsýslu og atvinnulífi. Upp úr því starfi var Öldungadeildin stofnuð árið 2004. Þar sat hann í öldungaráði meðan heilsan leyfði. Hann gerði einnig fyrstu útgáfu af Söguvef Öldungadeildar, sem síðar var komið fyrir á vefsetri SKÝ.

Foreldrar Odds voru Stefán Már Benediktsson verslunarmaður, f. 1906, d. 1945, og Sigríður Oddsdóttir læknaritari, f. 1907, d. 1988. Systkini hans eru Einar, f. 1931, Svala, f. 1934, Þóra, f. 1935, og Ragnheiður, f. 1939. Oddur kvæntist Hildi Hákonardóttur, f. 1938, árið 1955. Börn þeirra eru Kolbrún Þóra, f. 1956, og Hákon Már, f. 1958. Þau skildu. Oddur kvæntist Hólmfríði R. Árnadóttur, f. 1939, árið 1970. Börn hennar af fyrra hjónabandi eru Árni Geir Pálsson, f. 1963, og Kári Pálsson f. 1964. Saman eignuðust Oddur og Hólmfríður Guðrúnu, f. 1971, og Katrínu, f. 1977. Þegar þetta er ritað eru barnabörn Odds og Hólmfríðar samtals 13 auk eins barnabarnabarns.

Oddur var hugsjónamaður, frumkvöðull af köllun, atorkumaður sem ekki gafst upp þótt á móti blési, maður sem kom málum sínum fram með hæglátri ýtni fremur en ofsa. Auk þess sem að ofan getur lét hann víða til sín taka t.d. á sviði umhverfisverndar, persónuverndar og friðarmála. Oddur var mannvinur og mikill fjölskyldumaður. Hann var stofnandi og formaður Krabbameinsfélagsins Framfarar.

Megi minning hans lengi lifa.
Jóhann Gunnarsson

Valgerður Gunnarsdóttir, formaður Fókus og undirbúningsnefndar ráðstefnunnar

Þann 2.- 4. júní 2010 var haldin í fyrsta skipti á Íslandi alþjóðleg ráðstefna um upplýsingatækni í heilbrigðisþjónustu. Að ráðstefnunni stóðu EFMI – Evrópusamtök um upplýsingatækni í heilbrigðisþjónustu, Skýrslutæknifélag Íslands og Fókus – félag um upplýsingatækni í heilbrigðisþjónustu sem er faghópur innan Skýrslutæknifélagsins.

Ráðstefna um upplýsingatækni í heilbrigðisþjónustu

Yfirskrift ráðstefnunnar á ensku var EFMI Special Topic Conference 2010 Seamless Care – Safe Care The Challenges of Interoperability and Patient Safety in Health Care

Aðdragandi og undirbúningur

Undirbúningur fyrir ráðstefnuna hófst þegar árið 2007 þegar fulltrúaráð EFMI samþykkti umsókn Íslands um að fá að halda ráðstefnuna hér á landi. Fókus hafði þá verið félagi í EFMI frá árinu 2005.

Formleg undirbúningsnefnd fyrir ráðstefnuna var sett á laggirnar um mitt ár 2008 og í henni áttu sæti: Valgerður Gunnarsdóttir sem var formaður, Ásta St. Thoroddsen, varaformaður, Arna Harðardóttir, Ásgerður Magnúsdóttir, Benedikt Benediktsson, Óskar Einarsson, Hákon Sigurhansson og Rannveig Ásgeirsdóttir. Aðrir stjórnarmenn Fókus lögðu einnig sitt af mörkum. Framkvæmdastjóri Skýrslutæknifélagsins tók þátt í undirbúningi frá byrjun og átti sæti í undirbúningsnefnd. Á undirbúningstímanum voru alls þrír framkvæmdastjórar, fyrst Hólmfríður Arnardóttir, þá Pálína Kristinsdóttir og frá hausti 2009 var Arnheiður Guðmundsdóttir í nefndinni og bar hita og þunga af undirbúningnum.

Einnig var skipuð formleg dagskrárnefnd (Scientific Programme Committee) sem sá um skipulag faglegu dagskrárinnar og útgáfu bókar með fyrirlestrunum. Í henni áttu sæti Bernd Blobel sem var formaður, Ebba Þóra Hvannberg varaformaður, Jos Aarts, Christian Lovis, Jacob Hofdijk og Stig Kjær Andersen. Ebba Þóra var fulltrúi Íslands í nefndinni en aðrir nefndarmenn komu allir úr fulltrúaráði EFMI.

Auglýst var eftir erindum og tillögum um vinnusmiðjur og var frestur til loka janúar 2010. Erindin þurftu að uppfylla skilyrði um fagleg vinnubrögð og frágang. Þau voru prentuð hjá IOS útgáfunni í Hollandi og komu út í bók sem ráðstefnugestir fengu í hendur (ISBN 978-60750-562-4). Bókin er hluti af ritröð sem nefnist „Studies in Health Technology and Informatics“. Eintök af bókinni má finna í Þjóðarbókhlöðunni en erindin og veggspjöldin eru einnig birt á vefsíðu EFMI (www.efmi.org).

Bakhjarlar ráðstefnunnar og styrktaraðilar voru Heilbrigðisráðuneytið og Háskóli Íslands ásamt alþjóðasamtökunum GS1 og HL7 sem héldu sögulegan fyrsta samstarfsfund sinn í tengslum við ráðstefnuna. Einnig styrktu GS1 á Íslandi, EMR, Skýrr og Nýsköpunarmiðstöðin ráðstefnuna.

Tilgangur okkar var að ráðstefnan gæti nýst sem best þeim Íslendingum sem starfa að málefnum rafrænnar sjúkraskrár og við stefndum á þátttöku þverfaglegs hóps úr heilbrigðiskerfinu og stjórnsýslunni, nemenda og fræðimanna úr háskóla- og vísindasamfélaginu ásamt fólki úr hugbúnaðargeiranum og annars staðar úr atvinnulífinu.

Við vildum reyna að sameina bæði fræðilega umfjöllun og praktíska nálgun á málefnið og það tókst nokkuð vel.

Skipulag

Ráðstefnan var haldin á Háskólatorgi í tveimur stærstu fyrirlestrarsölunum með sýningarbása á ganginum fyrir framan. Þetta húsnæði reyndist einstaklega skemmtilegt og gott til ráðstefnuhalds og átt sinn þátt í því hve ráðstefnan tókst vel. Allt umhverfið á Háskólatorgi er fallegt og þægilegt.

Ráðstefnan var sett síðari hluta dags þann 2. júní og hófst með ávarpi heilbrigðisráðherra, Álfheiðar Ingadóttur. Einnig tóku formaður undirbúningsnefndar og forseti EFMI til máls og síðan var móttaka fyrir gesti í boði GS1 á Íslandi. Faglegi hluti ráðstefnunnar stóð svo í tvo heila daga, 3. og 4. júní í tveimur sölum með erindum, veggspjöldum og vinnusmiðjum. Hátíðarkvöldverður var haldinn í Perlunni á fimmtudagskvöldinu 3, júní og var hann vel sóttur og heppnaðist ágætlega.

Margir gestanna fóru í ferðir um landið eftir að ráðstefnunni lauk en við höfðum skipulagt ýmsar ferðir fyrir þá, m.a. ferð í Bláa lónið með kvöldmat á föstudagskvöldinu eftir ráðstefnulok og einnig 6 daga ferð um Ísland með heimsóknum á heilbrigðisstofnanir.

Þátttakendur voru um 180 talsins, þar af rúmlega 70 erlendir og yfir 100 Íslendingar. Var það framar okkar björtustu vonum en bæði bankahrun og eldgos höfðu sett nokkurt strik í áætlanir okkar á undirbúningstímanum.

Efni og dagskrá

Á ráðstefnunni var fjallað um úrlausnarefni við aukin rafræn samskipti í heilbrigðiskerfinu þ.e. samvirkni (e. interoperability) og þýðingu hennar fyrir öryggi sjúklinga.

Öryggi sjúklinga er m.a. háð því að heilbrigðisstarfsmenn geti haft aðgang að réttum upplýsingum um sjúklinga, á réttum tíma, óháð því hvar upplýsingarnar eru upprunnar. Greiður aðgangur að heilbrigðisupplýsingum þegar á þarf að halda er þannig eitt af undirstöðuatriðum þess hægt sé að veita rétta meðferð og koma í veg fyrir mistök. Gott upplýsingaaðgengi hefur því áhrif á gæði meðferðar og nýtingu fjármuna, en til þess að flæði upplýsinga sé gott þurfa mismunandi kerfi að geta talað saman eða með öðrum orðum þá þarf að vera samvirkni á milli þeirra.

Samvirkni heilbrigðiskerfa bæði innanlands og milli landa er þannig brýnt úrlausnarefni og á henni eru margar hliðar. Það þarf t.d. að huga að tæknilegum atriðum, gagnaöryggi, lagaramma, siðfræðilegum álitamálum og merkingarfræðilegri samvirkni (e. semantic interoperability) sem felur í sér að texti eða aðrar upplýsingar skila sér rétt á milli kerfa þannig að merking upplýsinga á áfangastað er sú sama og á upprunastað.

Alls bárust um 50 erindi. Þau voru send út til yfirlestrar hjá sérfræðingum um alla Evrópu sem völdu úr þá sem stóðust gæðakröfur. Alls voru 25 erindi samþykkt, 13 voru samþykkt sem veggspjöld og 3 sem vinnusmiðjur. Þar fyrir utan voru tvær vinnusmiðjur í boði dagskrárnefndarinnar, önnur þeirra haldin af verkefnisstjórum Evrópuverkefna um samþættingu og samvirkni heilbrigðisgagna og hin af GS1 og HL7 þar sem sérfræðingar ræddu um mismunandi notkun staðla og samræmingar fyrir samvirkni upplýsinga.

Tveir gestafyrirlesarar komu frá Bandaríkjunum. Þeir eru báðir mjög þekktir í faginu víða um heim. Annar þeirra var William Ed Hammond sem verið hefur um langt árabil formaður stjórnar HL7 staðlasamtakanna og er fumkvöðull í upplýsingatækni í Bandaríkjunum. Núna er hann framkvæmdastjóri miðstöðvar heilbrigðisupplýsingatækni hjá Duke háskóla.

Hinn aðalfyrirlesarinn var Peter L. Elkin prófessor við læknaskólann á Mount Sinai spítala í New York. Hann hefur unnið mikið við kóðunarkerfi og staðlagerð og rannsakað hvernig nota má heilbrigðisgögn í þróun og rannsóknum.

Þar fyrir utan voru þrír fyrirlesarar sem héldu inngangserindi fyrir sérstaka dagskrárhluta að beiðni dagskrárnefndarinnar. Þau voru Bernd Blobel sem talaði um hlutverk skipulags og uppbyggingar sjúkraskrár m.t.t. samvirkni, Ulrika Kreysa frá GS1 sem lýsti ferli merktra vara og íhluta og ræddi samvinnu GS1 og HL7 staðlasamtakanna og síðast en ekki síst María Heimisdóttir sem ræddi um rafræna sjúkraskrá og notkun klínískra vöruhúsa til að vinna upplýsingar fyrir stefnumótun og rekstur.

Dagskráin var sem sagt bæði þétt og áhugaverð og fólk var ákaflega ánægt með fyrirlesara og allt umhverfi ráðstefnunnar. Því er óhætt er að segja að hún hafi tekist vel og verið bæði Skýrslutæknifélaginu og Íslandi til sóma.

Síðan síðast...

Yfirlit yfir fundi og viðburði á vegum Ský veturinn 2009 – 2010

Yfir 20 viðburðir voru haldnir á vegum Ský síðastliðinn vetur og er það meira en nokkru sinni áður. Svo virðist sem áhugi á innlendum viðburðum sé mikill og var þátttaka almennt framar vonum. Það er því litið björtum augum á veturinn sem er framundan og verður lögð áhersla á metnaðarfulla dagskrá hjá félaginu.

Seinni hluti 2009

30. september	*Vefsöfnun*	Hádegisverðarfundur	Grand Hótel
14. október	*Lyklar að hraða og hagræðingu*	Hálfsdagsráðstefna	Grand Hótel
20. október	*Windows 7*	Örkynning	Engjateig
27. október	*Opinn hugbúnaður – eða ekki?*	Hádegisverðarfundur	Grand Hótel
12. nóvember	*Hugsun til hagnaðar*	Hálfsdagsráðstefna	Grand Hótel
17. nóvember	*Sjálfvirk vöktun tölvukerfa*	Örkynning	Engjateig
24. nóvember	*Hagræðing og hugsjónir*	Hálfsdagsráðstefna	Grand Hótel
24. nóvember	*Aðalfundur Fókus*	Aðalfundur	Grand Hótel
8. desember	*Ný sköpun á skjánum*	Hálfsdagsráðstefna	Grand Hótel
16. desember	*Hvað er spunnið í opinbera vefi?*	Hádegisverðarfundur	Grand Hótel

Fyrri hluti 2010

12. janúar	*Joomla örkynning*	Örkynning	Engjateig
2. febrúar	*Nýjungar í hugbúnaðargerð*	Hádegisverðarfundur	Grand Hótel
4. febrúar	*Aðalfundur ROÞ*	Aðalfundur	Engjateig
9. febrúar	*Aðalfundur Ský*	Aðalfundur	Engjateig
24. febrúar	*Öryggi og upplýsingar*	Hádegisverðarfundur	Grand Hótel
25. mars	*Mælikvarðar fyrir opinbera vefi*	Morgunverðarfundur	Grand Hótel
27. apríl	*Innri vefir*	Hádegisverðarfundur	Grand Hótel
28. apríl	*Aðalfundur faghóps um fjarskipti*	Aðalfundur	Engjateig
6. maí	*Stefnumót við faghópa Ský*	Fundur	Engjateig
10. maí	*Nytsemi á hlaupum*	Örkynning	Engjateig
20. maí	*UT-Dagurinn*	Hálfsdagsráðstefna	Salurinn Kópavogi
2. – 4. júní	*EFMI STC 2010*	2ja daga ráðstefna	Háskólatorg HÍ

Rétt er að minna á að hægt er að nálgast upplýsingar um liðna atburði og glærukynningar frá þeim á vefnum okkar www.sky.is undir „Liðnir atburðir“.






...framundan

Starfsemin í vetur

Dagskrá Ský fram að áramótum er í mótun og eru hér fyrstu drög að henni. Gera má ráð fyrir að fleiri viðburðum verði bætt inn eftir óskum og aðstæðum, sérstaklega þó örkynningum sem hafa mælst vel fyrir. Viðburðir faghópa verða auglýstir sérstaklega innan hvers faghóps.

Við hvetjum félagsmenn Ský til að setja sig í samband við skrifstofuna hafi þeir áhuga á að taka virkan þátt í starfi faghópa eða undirbúningi viðburða. Við minnum félagsmenn einnig á að hægt er að skrá sig í og úr faghópum með því að vera í sambandi við skrifstofuna. Yfirlit yfir faghópa er að finna á vefsíðunni www.sky.is

Seinni hluti 2010 – drög að dagskrá

22. september	Samskiptamiðlarnir FaceBook, Twitter og LinkedIn	Örkynning
5. október	Skjalamál og vinnureglur	Hádegisverðarfundur
19. október	NordiCHI 2010 í samstarfi við HR og HÍ	Ráðstefna
19. október	Kæling tölvusala	Örkynning
27. október	Hagræðing með „Virtualization“	Hádegisverðarfundur
23. nóvember	Hugbúnaðarráðstefna	Ráðstefna
25. nóvember	Aðalfundur Fókus	Fundur
8. desember	Viðskiptahugbúnaður	Ráðstefna

Eftir áramótin er stefnt að því að halda sama striki með fjölbreyttu úrvali viðburða ásamt aðalfundi Ský sem verður í febrúar.

Ath: Fylgist vel með á vefsíðunni okkar www.sky.is þar sem efni og tímasetningar atburða geta breyst.

Frá skrifstofu Ský

Frá því í ágúst 2009 hefur einungis framkvæmdastjóri félagsins, Arnheiður Guðmundsdóttir, verið starfandi á skrifstofunni í stað tveggja starfsmanna síðustu ár.

Starfsemin var þó mjög lífleg síðasta vetur og voru haldnir rúmlega 20 viðburðir á vegum Ský. Stærsti viðburðurinn var alþjóðleg ráðstefna um heilbrigðismál, EFMI STC 2010, sem haldin var á Íslandi í byrjun júní í samstarfi við EFMI (Evrópusamtök um upplýsingatækni í heilbrigðisþjónustu). Átti faghópurinn Fókus allan heiður af undirbúningi hennar í samvinnu við skrifstofuna. Einnig voru margir aðrir stórir viðburðir svo sem UT-dagurinn, fjöldi örkynninga, hádegisverðar- og morgunfunda ásamt hálfsdagsráðstefnum.

Faghópar Ský eru mjög fjölbreyttir og er hugmyndin á bakvið þá að safna saman félagsmönnum sem eru sérfræðingar í, eða hafa áhuga á, því málefni sem faghópurinn sérhæfir sig í. Faghóparnir koma að félagsstarfinu með mismunandi hætti en flestir taka þátt í undirbúningi stærri viðburða á vegum Ský ásamt því að halda minni viðburði fyrir þá sem skráðir eru í viðkomandi faghóp. Vert er að benda á að hægt er að skrá sig í marga faghópa, en aðild að þeim er hluti af félagsstarfinu. Stofnun faghóps um hugbúnaðargerð og faghóps tækni- og kerfisstjóra hefur verið rædd og ef þú lesandi góður hefur áhuga á að vera með í undirbúningi þeirra eða stofna faghóp um önnur málefni tengd upplýsingatækni er um að gera að setja sig í samband við skrifstofuna.

Stjórn félagsins fór í gegnum stefnumótunarferli með nemum í MBA námi við Háskóla Íslands síðastliðinn vetur og mun þeirri vinnu ljúka nú í haust. Tilgangur stefnumótunarvinnunnar er fyrst og fremst að staldra við og fara yfir starfsemi félagsins ásamt því að fastsetja markmið og framtíðarsýn þess. Stjórnir faghópanna tóku virkan þátt í vinnunni og voru haldnir hugarflugsfundir með þeim til að ná fram sem flestum sjónarmiðum um starfsemi Ský. Þar komu fram margar áhugaverðar hugmyndir sem tekið verður mið af við mótun á framtíð félagsins.

Ný stjórn var kosin í febrúar og er Sigrún Gunnarsdóttir nú formaður Ský. Úr stjórn gengu Elín Gränz og Ásrún Matthíasdóttir og er þeim þakkað fyrir þau ár sem þær hafa setið í stjórninni. Félagið nýtur þó krafta Ásrúnar áfram þar sem hún er í ritnefnd Tölvumála.

Sigrún Gunnarsdóttir formaður

Fráfarandi formaður, Magnús Hafliðason gaf kost á sér áfram í stjórn, og eru honum þökkuð vel unnin störf sem formaður. Aðrir í stjórn eru: Ragnheiður Magnúsdóttir, Bjarni Sigurðsson, Hjörtur Grétarsson, Þórhildur Hansdóttir Jetzek, Jón Heiðar Þorsteinsson og Sigurður Friðrik Pétursson.

Veturinn framundan verður spennandi og er mikill hugur í fólki að halda uppi metnaðarfullu starfi með fjölda viðburða. Hikið ekki við að hafa samband við skrifstofu Ský varðandi félagsstarfið.

Tölvukerfin eiga heima hjá **Skýrr**

Skýrr hýsir og rekur netþjóna og tölvukerfi fyrirtækja af öllum stærðum og gerðum:

Sveitarfélagið Vogar

Öll starfsemi sveitarfélagsins, hvort sem um er að ræða grunnskólann eða íþrótta-miðstöðina, stólar á tölvukerfi hjá Skýrr.

Bílabúð Benna

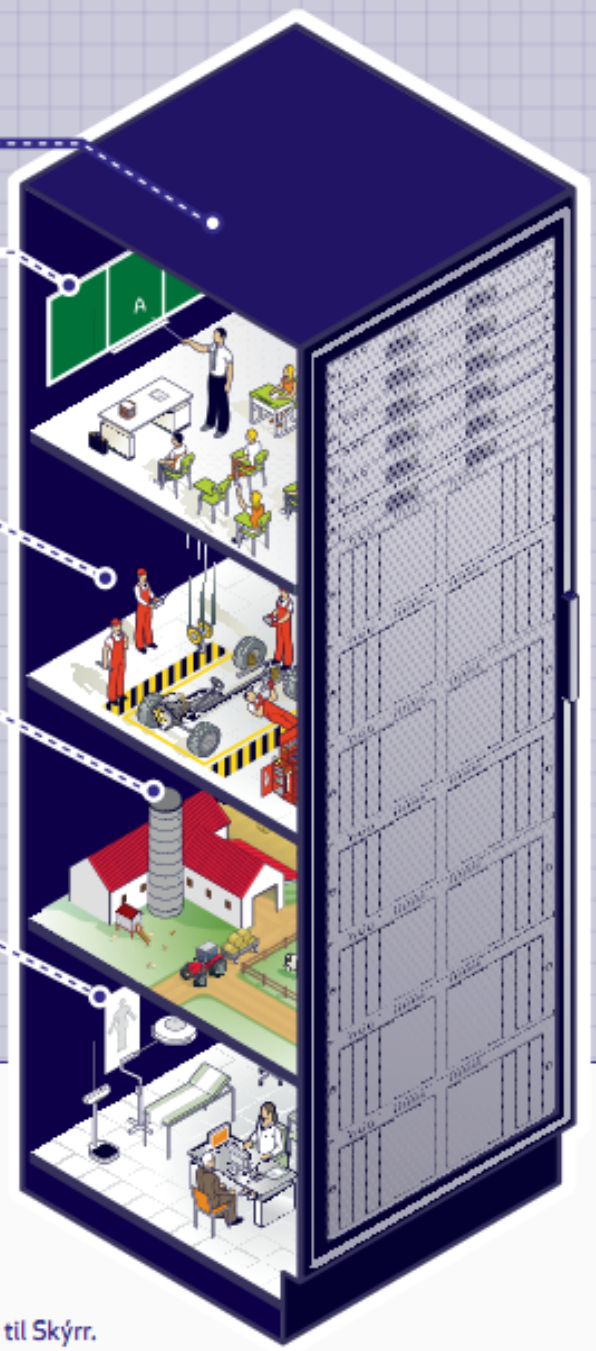
Bílabúð Benna treystir á öruggt aðgengi að ökutækjaskrá allra bifreiða á Íslandi í gegnum Upplýsingaheima Skýrr.

Bændasamtökin

Bændasamtökin belta sér fyrir málefnum bænda og þurfa ekki að hafa áhyggjur af tölvumálum á meðan.

Lækning

Trúnaðarupplýsingar eru í öruggu skjóli bak við traustan eldvegg Skýrr.



Hjá Skýrr starfa 340 sérfræðingar sem sjá um að hýsa, reka og þjónusta tölvukerfi fyrirtækja af öllum stærðum og gerðum.

Þau fyrirtæki sem hafa flutt tölvukerfin til okkar hafa minnkað umstang, aukið öryggi og dregið verulega úr kostnaði.

Kannaðu hvort það borgi sig ekki að flytja tölvukerfið til Skýrr.

569 5100
skyrr@skyrr.is

SKÝRR
Velkomin