TÖLVUMÁL

TÍMARIT SKÝRSLUTÆKNIFÉLAGS ÍSLANDS / 1.TBL / 42. ÁRGANGUR / NÓVEMBER 2017

ÓGNIR DAGSINS Í DAG OG LAUSNIR TIL FRAMTÍÐAR

Persónuvernd
Skýjagleypir
Veikasti hlekkurinn
Staðalímyndir
Samskiptablekking

/ ský /

/ ský /

Tímaritið Tölvumál
Fagtímarit um upplýsingatækni.
Tölvumál hafa verið gefin út frá
árinu 1976 af Skýrslutæknifélaginu.

Prentvinnsla
Litlaprent ehf.

Ritstjóri og ábyrgðarmaður
Ásrún Matthíasdóttir

Aðrir í ritstjórn
Ágúst Valgeirsson
Sigurjón Ólafsson
Eyjólfur Ingi Ásgeirsson
Atli Týr Ægisson

Skýrslutæknifélag Íslands
Ský, er félag einstaklinga,
fyrirtækja og stofnana á sviði
upplýsingatækni.

Starfsmenn Ský
Arnheiður Guðmundsdóttir,
framkvæmdastjóri
Hildur Rut Halblaub

Stjórn Ský
Guðjón Karl Arnarson, formaður
Snæbjörn Ingi Ingólfsson
Theódór R. Gíslason
Birna Íris Jónsdóttir
Kristján Ólafsson
María Ingimundardóttir
Díana Dögg Víglundsdóttir

Aðsetur
Engjateigi 9
105 Reykjavík
Sími: 553 2460
www.sky.is I sky@sky.is

Blaðið er gefið út í 1.200 eintökum.
Áskrift er innifalin í félagsaðild að Ský.
Þökkun blaðsins fer fram í vinnustofunni Ás.
Prentvinnsla Litlaprent ehf.

RITSTJÓRNARPISTILL

Dr. Ásrún Matthíasdóttir, ritstjóri Tölvumála

Ógnir dagsins í dag og lausnir til framtíðar er þema Tölvumála í ár og er margar áhugaverðar greinar að finna í blaðinu. Fjallað er um gagnagrunna, *Internet of things*, nýjar persónuverndarreglur, tölvuinnbrot og samstarf lögreglu og einkageirans svo eitthvað sé nefnt, en einnig annað efni eins og gervigreind, sannlíki og staðalímyndir.

Það er hægt að hegða sér óæskilega á netinu á ýmsan hátt hvort sem við erum að tala t.d. um tölvuinnbrot, stuld á persónueinkennum eða neteinelti. Sífellt er verið að vinna að betri vörnum og vinnuferlum, en það er alveg sama hvað tæknin og hugbúnaðurinn er fullkominn, notandinn kemur alltaf inn sem áhættuþáttur, s.s. þegar kemur að dreifingu á efni og aðgengi. Mannlegi þátturinn skiptir miklu máli þegar við tökumst á við ógnir og lausnir.

Við notum snjalltæki mikið í dag og teystum orðið á þau næstum því í blindni. Stór hluti af lífi margra, sérstaklega yngra fólks, fer fram með þessum tækjum. Við treystum á þessi tæki til að ná okkur í upplýsingar og hafa samskipti en einnig til að geyma fyrir okkur gögn.

Tengt þessu langar mig að segja frá ungum manni sem var nýlega með foreldrum sínum í erlendri stórborg. Fjölskyldan hafði leigt íbúð og var nýkomin á staðinn. Um kvöldið voru þau í góðra vina hópi en foreldrarnir ákváðu að fara fyrr heim og ætlaði hann að fylgja á eftir í leigubíl. Mamman sendi honum heimilisfangið í símann og tveim tímum seinna fengu þau skilboð um að hann væri á leiðinni. Síðan leið og beið, ekki kom hann og voru þau orðin ansi áhyggjufull þegar nær klukkutími var liðinn. Hann svaraði ekki síma, ekki skilaboðum eða tölvupósti. Systir hans var vakin heima á Íslandi til að senda skilaboð í gegnum öpp sem foreldrarnir nota ekki en ekkert gerðist, hann svaraði ekki en samt virtist síminn nettengdur. Það geta örugglega margir getið sér til um þær hugsanir sem fóru um huga þeirra á þessum tíma. Tveimur tímum seinna fann pabbinn unga manninn á gangi um hverfið í leit að húsinu. En hvað hafði gerst? Um leið og hann sendi skilaboðin um að hann væri að stíga inn í leigubíl missti hann símann og skjáborðið brotnaði alveg í mask. Hann gat ekkert gert, engu svarað, ekkert skoðað, náði ekki í neitt í símanum og gat ekki látið vita af sér. Hann fann því ekki heimilisfangið sem hann hafði fengið í SMSi og átti líka í tölvupósti. Enga aðstoð var að hafa hjá leigubílstjórum eða á opnum veitingastöðum, enginn vildi hringja fyrir hann eða lána honum síma (sem er efni í annan pistil). Eina sem hann gat gert var að láta keyra sig að íslenska sendiráðinu sem hann vissi að var í nágrenni íbúðarinnar og ganga af stað í þeirri von að finna húsið. Þarna hefði verið betra að hafa heimilisfangið skrifað á miða.

„It is only when they go wrong that machines remind you how powerful they are“ Clive James

EFNISYFIRLIT

VILTU GANGA Í SKÝ?

Skýrslutæknifélag Íslands, í daglegu tali nefnt Ský, er félag einstaklinga, fyrirtækja og stofnana á sviði upplýsingatækni. Ský er rekið án hagnaðarmarkmiða og starfa tveir starfsmenn í 1.5 stöðugildi hjá félaginu.

Aðild er öllum heimil og bjóðum við ungt fólk í tölvugeiranum sérstaklega velkomið.

Starfsemi félagsins er aðallega fólgin í, auk útgáfu Tölvumála, að halda fundi og ráðstefnur um sérhæfð efni og nýjungar í upplýsingatækni. Félagið á og heldur UTmessuna sem er einn stærsti viðburður í tölvugeiranum á Íslandi. Einnig veitir félagið Upplýsingatækniverðlaunin árlega frá 2010. Ský sér um að halda Bebras tölvuáskoruninia árlega í skólum landsins en það er alþjóðlegt verkefni sem hvetur krakka til að nota hugsunarhátt forritunar við lausn á skemmtilegum verkefnum. Félagið stóð að ritun og samantekt á „Sögu tölvuvæðingar á Íslandi 1964-2014“ og er hún á vef Ský. Ýmis önnur starfsemi tengd tölvu- og tæknigeiranum fer fram hjá Ský enda félagið óháð öllum.

Tilgangur Ský er að miðla þekkingu milli þeirra sem starfa við eða hafa áhuga á upplýsingatækni.

Hlutverk Ský er að bjóða uppá fjölbreytta og metnaðarfulla viðburði í formi fræðslufunda og ráðstefna um upplýsingatækni og hlúa að því öfluga þekkingar- og tengslaneti sem myndast hefur innan félagsins og veita þannig félagsmönnum sínum virðisauka og vegsemd.

MARKMIÐ SKÝ ERU:

- að breiða út þekkingu á upplýsingatækni og stuðla að skynsamlegri notkun hennar
- að skapa vettvang fyrir faglega umræðu og tengsl milli félagsmanna
- að koma fram opinberlega fyrir hönd fólks í upplýsingatækni
- að stuðla að góðu siðferði við notkun upplýsingatækni
- að styrkja notkun íslenskrar tungu í upplýsingatækni

INNAN SKÝ FJÖLMARGIR FAGHÓPAR OG GETUR FÓLK SKRÁÐ SIG Í ÞÁ SEM HENTA:

- Faghópur um vefstjórnun
- Faghópur um rafræna opinbera þjónustu
- Faghópur um öryggismál
- Faghópur um fjarskiptamál
- Faghópur um hugbúnaðargerð
- Faghópur um rekstur tölvukerfa
- Faghópur um menntun, fræðslu og fræðistörf í UT
- Fókus, faghópur um upplýsingatækni í heilbrigðisþjónustu
- Öldungadeild, ætlaður þeim sem hafa starfað lengur en 25 ár í UT geiranum

ÁVINNINGUR AF FÉLAGSAÐILD:

- Lægri ráðstefnugjöld á ráðstefnur félagsins fyrir félagsmenn
- Áskrift að Tölvumálum, fagtímariti með efni tengdu tölvunotkun og upplýsingatækni
- Leið að faghópastarfi innan félagsins
- Hafi félagsmenn áhuga á að stofna faghóp eða tengslanet myndi félagið aðstoða við það
- Félagsmönnum er gefið tækifæri til að starfa í/með undirbúningsnefndum ráðstefna og funda félagsins
- Tengslanet, fræðsla, tengslanet, fræðsla, tengslanet ...

NÁNARI UPPLÝSINGAR ER AÐ FINNA Á WWW.SKY.IS OG HJÁ SKRIFSTOFU SKÝ.

WORKPLACE FRÁ FACEBOOK OG PERSÓNUVERND

Viðtal við Vigdísi Evu Líndal, Persónuvernd
Viðtalið tók Sigurjón Ólafsson

Eins og margir hafa orðið áskynja þá hefur Workplace frá Facebook náð mikilli útbreiðslu á undraskömmum tíma hér á landi og í reynd stuðlað að ákveðinni byltingu í innri upplýsingamiðlun og samskiptum starfsmanna á vinnustöðum. Hvaða áhrif, ef einhver, hefur innleiðing Workplace á persónuvernd starfsmanna?

HVAÐ ER WORKPLACE?

Workplace er samfélagsmiðill og hugbúnaður fyrir innri vefmiðlun í fyrirtækjum. Tilgangurinn er ekki síst að auka flæði upplýsinga og þekkingar, styrkja samvinnu og skilvirkni, færa starfsfólk nær hvert öðru og efla starfsanda á vinnustað. Workplace er sagt fækka tölvupóstum og fundum ásamt því að samskipti fólks verða einfaldari og fljótlegri. Það virkar í öllum megin atriðum eins og Facebook en er þó alveg aðskilið í rekstri. Starfsmenn þurfa t.d. ekki að vera á Facebook til að tengjast Workplace.

Eimskip var fyrsta íslenska fyrirtækið sem innleiddi Workplace (hét þá Facebook at Work) í apríl 2016. Síðan þá hefur fjöldi fyrirtækja fylgt í kjölfarið t.d. Icelandair, Landspítali, Hafnarfjörður, Dominos og Landsnet. Talið er að um 2-300 íslenskir vinnustaðir hafi tekið hugbúnaðinn í notkun og ekkert lát virðist vera á þessari þróun. Samkvæmt tölum frá Facebook hafa alls hafa um 30.000 fyrirtæki innleitt Workplace á sama tíma og höfðatalan því merkileg eins og svo oft áður þegar Íslendingar eru annars vegar. Við Íslendingar erum spennt fyrir nýjungum og erum fljót að taka ákvarðanir. En höfum við farið of geyst? Þarf að e.t.v. að staldra við og hugsa málin til enda?

Vigdís Eva Líndal, skrifstofustjóri upplýsingaöryggis Persónuverndar, er sérfróð um persónuvernd og hefur fengist við þessi mál innan stofnunarinnar. Við fengum hana í viðtal.

HVERNIG KOM WORKPLACE INN Á BORÐ PERSÓNUVERNDAR?

„Persónuvernd hefur nú til meðferðar nokkur frumkvæðismál en upphaf þeirra má rekja til frétta um að fyrirtæki á Íslandi væru að taka í notkun Workplace. Aðrar persónuverndarstofnanir í nágrannalöndunum hafa verið að skoða Workplace og gefið út leiðbeiningar um hverju þurfi að huga að þegar lausnin er tekin í notkun. Norska persónuverndarstofnunin, Datatilsynet, hefur t.d. gefið út leiðbeiningar um notkun Workplace. Af þeirri ástæðu töldum við okkur m.a. skylt að skoða þessi mál nánar hér á Íslandi.“

HVAÐ BER HELST AÐ HAFA Í HUGA VIÐ INNLEIÐINGUNA AÐ MATI PERSÓNUVERNDAR?

„Áður en ég fjalla sérstaklega um Workplace þá eru nokkur atriði sem fyrirtæki þurfa alltaf að hafa í huga í sambandi við persónuvernd þegar gerðir eru samningar um innleiðingu og notkun á hugbúnaði. Þetta eru tveir aðilar, annars vegar ábyrgðaraðili, þ.e. fyrirtæki eða stofnun, og síðan vinnsluaðili, t.d. upplýsingatæknifyrirtæki, eða í þessu tilviki Facebook. Til að ábyrgðaraðili geti ráðið vinnsluaðila þarf hann fyrst að ganga úr skugga um að vinnsluaðilinn geti framkvæmt viðeigandi öryggisráðstafanir og hvort sett hafi verið öryggisstefna og áhættumat framkvæmt.

Þegar hann er búinn að því og vinnsluaðilinn uppfyllir öll þau skilyrði sem ábyrgðaraðilinn gerir til öryggis upplýsinganna þá fyrst getur hann gengið til samninga við hann og gert s.k. vinnslusamning, þar sem fyrirmæli ábyrgðaraðilans til vinnsluaðilans eru skjalfest. Persónuverndarlögin gera kröfu um að gerður sé sérstakur vinnslusamningur, þ.e. samningur um vinnslu persónuupplýsinga. Í framkvæmd hefur það oft verið svo að sá leikur er ójafn, ábyrgðaraðilinn hefur lítið um það að segja hvað stendur í samningnum og hvaða upplýsingar eru afhentar. Það breytir því þó ekki að höfuðábyrgðin liggur á ábyrgðaraðilanum ef eitthvað fer úrskeiðis við vinnsluna. Þegar utanaðkomandi aðili er fenginn til að sinna tiltekinni vinnslu fyrir ábyrgðaraðila, s.s. með því að bjóða fram tiltekinn hugbúnað, er yfirleitt fyrst horft á hvort vinnslusamningur sé til staðar og hvað kemur fram í honum. Eftir því sem upplýsingarnar eru viðkvæmari, t.d. upplýsingar um heilsufar eða refsiverðan verknað, því meiri kröfur þarf að gera til bæði vinnsluaðilans og vinnslunnar sjálfrar.

Hvað varðar Workplace þá þarf að skoða nokkur atriði hverju sinni. Í fyrsta lagi þarf að kanna hvort að vinnslusamningur hafi verið gerður við Facebook, að undangengnu mati á þeim öryggisráðstöfunum sem eru viðhafðar hjá því fyrirtæki. Almennt hefur það verið svo að hugbúnaðurinn virðist eingöngu vera ætlaður sem nokkurs konar innri vefur og ekki til að miðla á milli starfsmanna viðkvæmum persónuupplýsingum. Að því marki sem eingöngu er verið að miðla almennum upplýsingum þá má segja að ekki séu gerðar jafn strangar kröfur til efnis vinnslusamninga og undanfarandi aðgerða og ef um væri að ræða upplýsingakerfi sem héldi utan um viðkvæmar persónuupplýsingar.

Í öðru lagi þarf að huga að þeirri fræðslu sem starfsmenn fá þegar hugbúnaðurinn er tekinn í notkun. Persónuverndarlögin gera að skilyrði við vinnslu persónuupplýsinga að einstaklingar fái tiltekna fræðslu um

hana. Það má í raun segja að í þessu endurspeglist annað meginstef laganna – gagnsæi. Hitt er sjálfsákvörðunarrétturinn. Grundvallarhugsunin á bak við fræðslu er sú að ef starfsmaðurinn veit ekki hvaða upplýsingum Facebook er að safna um hvað hann gerir inn á Workplace, og hvernig vinnustaðurinn síðan vinnur úr þeim upplýsingum, þá gæti orðið ansi erfitt fyrir hann að njóta réttinda sinna, t.a.m. rétt til að andmæla vinnslu, fá upplýsingar leiðréttar eða þeim jafnvel eytt.“

HVERNIG FER ÞESSI ATHUGUN PERSÓNUVERNDAR FRAM?

„Það er ýmislegt sem getur þurft að kanna í athugunum sem þessum. Fyrst og fremst beinast þær að því að fá góða mynd af þeirri vinnslu persónuupplýsinga sem fer fram með notkun Workplace, t.a.m. hvaða persónuupplýsingar sé verið að vinna með, t.d. hvort eingöngu er um að ræða upplýsingar um starfsmenn eða er einnig verið að vinna með upplýsingar um einstaklinga sem eru í viðskiptum, efni vinnslusamnings og hvaða fræðsla var veitt áður en hugbúnaðurinn var tekinn í notkun. Hér er mjög mikilvægt að hafa í huga hvers konar upplýsingar er verið að vinna með hugbúnaðinum. Annars vegar þarf að skoða hvaða upplýsingar starfsmennirnir setja inn og hins vegar hvort og að hvaða marki Facebook safnar upplýsingum um hegðun þeirra inni á Workplace. Þetta getur skipt miklu máli upp á hversu ítarleg fræðslan þarf að vera.

Persónuvernd leggur mikla áherslu á að stigið sé varlega til jarðar. Áður en fyrirtæki fara af stað við að taka í notkun nýjan hugbúnað, t.d. eins og Workplace, þá þarf alltaf að gera áhættumat. Gerð áhættumats felur í sér, í mjög stuttu máli, að meta hver sé áhættan við ganga til samninga við tiltekið fyrirtæki um tiltekna vinnslu fyrir sig og að meta hvaða áhætta sé ásættanleg og hver sé óásættanleg. Hversu ítarlegt þetta áhættumat á að vera, fer líka eftir tegundum upplýsinganna. Eftir því sem persónu-upplýsingarnar eru viðkvæmari, því ítarlegra þarf matið að vera. Hvað varðar Workplace þá er í mörgum tilvikum um að ræða vistun upplýsinga í tölvuskýi og þá skiptir efni vinnslusamnings miklu máli, m.a. hvort vista megi upplýsingar í skýi og þá í hvaða landi. Það er eitt að senda gögn til Írlands, sem er hluti af EES-svæðinu, eða hvort verið er að flytja til Bandaríkjanna. Facebook er í dag á s.k. „Privacy Shield“ lista bandarískra viðskiptaráðuneytisins, en það þýðir að heimilt er að senda upplýsingar frá Evrópu til þeirra fyrirtækja í Bandaríkjunum sem hafa fengið skráningu á þennan lista. Það breytir því þó ekki að margir hafa miklar efasemdir um að öryggi persónuupplýsinga sé nægilega tryggt þegar slíkar upplýsingar eru sendar til Bandaríkjanna, þar sem almennt gilda þar allt aðrar reglur og yfirvöld hafa meiri heimildir til að fá aðgang að persónuupplýsingum.

Auk áhættumats er eðlilegt að fram fari stefnumótun um notkun Workplace áður en hugbúnaðurinn er tekinn í notkun. Í því felst að fyrirtæki þurfa að ákveða hvaða upplýsingar eigi að setja þarna inn, fara yfir hvert þær eru að fara og setja síðan verklagsreglur hvað má og hvað ekki. Í framhaldi þarf svo að vera fræðsla til starfsmanna um þessar verklagsreglur og stefnumótunina.

Þetta eru því meginatriðin sem við erum að skoða, þ.e. tegundir persónuupplýsinga sem unnið er með, efni vinnslusamninga og fræðslu til starfsmanna og/eða viðskiptavina. Sú framkvæmd er í raun í fullu samræmi við það sem önnur persónuverndaryfirvöld, t.d. Datatilsynet í Noregi, hafa verið að gera í sínum leiðbeiningum.

Það er líka mikilvægt að hafa í huga að þetta þarf alls ekki að vera bannað en það þarf að fylgja ákveðnum reglum. Það þarf líka að hafa í huga að það eru ákveðnar skyldur á opinberum stofnunum um skjalavistun gagnvart Þjóðskjalasafni og héraðsskjalasöfnum og þeim spurningum þarf að vera búið að svara áður en þetta er tekið í gagnið, t.d. hvernig er farið með gögn sem verða til– hvílir skilaskylda á viðkomandi stofnun um þær upplýsingar sem safnast inni á Workplace og hvernig er rekjanleika háttað í tengslum við ákvarðanatöku?

Í stuttu máli má segja að ef það eru til staðar skýrar verklagsreglur og fræðsla er góð þá eru mun minni líkur á að það sé misfarið með upplýsingar. Starfsmönnum getur t.d. fundist óþægilegt að það séu upplýsingar eins og myndir og um stöðu þess i fyrirtækinu og því þarf að gera þeim grein fyrir hvað þetta þýðir og hvaða valmöguleikar eru í boði. Þarna er líka mjög mikilvægt að hafa í huga að allar upplýsingar, sem hægt er að tengja við starfsmanninn, t.d. myndir, stöðu innan fyrirtækis, samskipti hans við aðra starfsmenn o.s.frv. falla undir hugtakið persónuupplýsingar.

Í þessu sambandi er líka vert að nefna að í maí 2018 er væntanleg ný löggjöf í Evrópu um persónuvernd (GDPR) sem gerir mun ríkari kröfur til öryggis við meðhöndlun og vörslu persónuupplýsinga í stjórnun og rekstri hjá bæði einkafyrirtækjum og opinberum aðilum. Þessi löggjöf leggur mun ríkari skyldur á vinnsluaðilann, án þess þó að dregið sé úr skyldum ábyrgðaraðilans. Með tilkomu hinnar nýju löggjafar fær vinnsluaðili sjálfstæðar skyldur sem hann þarf að huga að. Í því felst m.a. að ef eitthvað kemur upp varðandi vinnslu persónuupplýsinga þá er ekki bara hægt að benda á fyrirtækið (ábyrgðaraðilann) heldur ber vinnsluaðilinn, í þessu tilviki Facebook, einnig sjálfstæða ábyrgð á að sú vinnsla sem fram fer hjá honum sé í samræmi við nýju löggjöfina.“

HAFIÐ ÞIÐ FENGIÐ EINHVERJAR KVARTANIR FRÁ STARFSMÖNNUM Í FYRIRTÆKJUM ÞAR SEM WORKPLACE HEFUR VERIÐ INNLEITT?

„Nei, Persónuvernd hafa ekki ennþá borist kvartanir frá starfsmönnum fyrirtækja sem hafa tekið Workplace í notkun. Þó hafa borist nokkrar fyrirspurnir frá starfsmönnum þar sem óskað hefur verið eftir leiðbeiningum um hvernig sé best að haga samskiptum við vinnuveitendur til að fá upplýsingar o.s.frv. Við höfum líka fengið fyrirspurnir frá stofnunum sem hafa áhuga á að taka í notkun Workplace og vilja fá leiðbeiningar og það er hið besta mál. Nú er unnið að því hér að gefa út leiðbeiningar um Workplace og þær verða birtar innan skamms, vonandi áður en blaðið kemur úr prentun. Stefnan þar er sú að hafa þær hagnýtar og ekki of flóknar, þannig að allir skilji.

Hlutverk Persónuverndar er að standa vörð um friðhelgi einkalífsins og persónuvernd. Það er oft ákveðinn misskilningur uppi um að Persónuvernd vilji banna nýjar leiðir til að vinna persónuupplýsingar en í raun snýst þetta ávallt um að ganga úr skugga um að staðið sé vörð um réttindi einstaklinganna og að fara að þeim skyldum sem á fyrirtæki eru lögð, ásamt því að sjálfsákvörðunarréttur einstaklinga og gagnsæi við vinnslu sé tryggt. Þannig að, eins og segir í nýju löggjöfinni sem væntanleg er á næsta ári – „vinnsla persónupplýsinga ætti að hafa það að markmiði að þjóna mannkyninu“, sem má segja að feli í sér að mannkynið á ekki að vera þræll tækninnar, heldur að nýta hana sér til hagsbóta.“

Það verður fróðlegt að fylgjast áfram með þróun Workplace hér á landi og auðvitað er fyllsta ástæða til að hvetja fyrirtæki til að taka tillit til væntanlegra leiðbeininga sem Persónuvernd er með í smíðum.

ÓGNIR GAGNAGRUNNA Í NETVÆDDUM VIÐSKIPTUM NÚTÍMASAMFÉLAGS

HUGVEKJA GAGNAGRUNNS SÉRFRÆÐINGS

Tómas Helgi Jóhannsson, gagnagrunnsstjóri hjá RB

Tækniumhverfi í nútímasamfélagi hefur tekið miklum breytingum og ef bara er litið til síðustu áratuga þá er breytingin geysileg. Í augum margra, sérstaklega af eldri kynslóðinni, er hún í senn ógnvekjandi og yfirþyrmandi en einnig spennandi. Sem betur fer taka langflestir þessum tækniframförum fagnandi og bókstaflega gleypa tæknina í sig. Dæmi um nýjungar sem í dag þykja orðið sjálfsagðar eru að versla á Internetinu sem og að eiga bankaviðskipti við sinn viðskiptabanka á þeim vettvangi. Þessi viðskipti hafa síðan teygt anga sína í farsímana með tilheyrandi „þægindum“ fyrir alla.

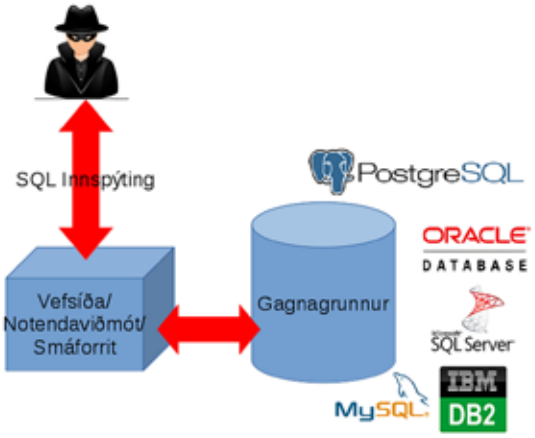
En að baki allra vefverslanakerfa, netbanka og smá-forrita (e. apps), sem tengjast verslun eða banka, er einhver gagnagrunnur. Gagnagrunnur sem heldur utan um öll viðskipti einstaklinga við viðkomandi verslun eða banka. Þessar upplýsingar eru persónugreinanlegar og því afar viðkvæmar og lúta því persónuverndarlögum og bankaleynd þar sem það á við.

ÞRÓUN GAGNAGRUNNA OG FORRITUNARMÁLA UNDANFARNA ÁRATUGI

Gagnagrunnar hafa undanfarinn áratug tekið gríðarlegt stökk í þróun, afkastageta þeirra hefur margfaldast sem og viðhald og annað utanumhald orðið betra samhliða auknu flækjustigi. Þetta hefur orðið til þess að margvíslegir möguleikar í forritun með SQL fyrirspurnamálinu hafa litið dagsins ljós. M.a. eru möguleikar á að varpa gögnum úr einu formi í annað, áður en gögnunum er skilað til forrits, mun fjölbreyttari í dag en áður. Það sem er nýjast og heitast í dag er vörpun úr töfluformi (e. relational) yfir í JSON (e. Javascript Object Notation) til að geta flutt gögn yfir í snjallsíma með auðveldum og hraðvirkum hætti. En þessar framfarir hafa líka orðið til þess að það, að skrifa SQL fyrirspurn og/eða gagnagrunns-forrit (gagnagrunns-pakka) er mun vandmeðfarnara en áður.

Eins hefur þróun margra forritunarmála eins og Java, JavaScript, PHP, Ruby, ASP.Net, Python, C og C++ (að ógleymdum öðrum forritunarmálum sem ekki verða talin upp hér) einnig orðið gríðarleg fyrir forritun vef-, bakvinnslu- og smá-forrita og mögulegur stuðningur við ótal mismunandi gagnagrunna aukist frá því sem áður var.

Samfara þessum framförum, sem nefndar eru hér að framan, og með tilkomu vefverslanakerfa, netbanka, banka- og verslunarforrita fyrir farsíma (e. mobile apps) hafa kröfur um hraðvirkar SQL-fyrirspurnir sem og aðra gagnavinnslu fengið aukið vægi. Framleiðendur gagnagrunna hafa, að sama skapi, verið duglegir að koma fram með nýjungar er styrkja það sem glímt er við enn frekar. Sú þróun hefur oft í för með sér að flóknar beinlínu- og/eða Internet-tengdar (e. online) SQL-fyrirspurnir sem geta tekið einhverjar sekúndur með eldri SQL-rithætti detta undir sekúndu í keyrslu með nýrri SQL-rithætti og bakvinnslur í gagnagrunnum sem áður tóku mínútur uppí margar klukkustundir geta hæglega dottið niður í fáeinar sekúndur.



SQL innspýting.

HVERJAR ERU ÞÁ HELSTU ÓGNIR GAGNAGRUNNA?

Segja má að ein stærsta ógn gagnagrunna í dag sé sú að forritarar nýti ekki til fulls þær nýjungar, sem framleiðendur gagnagrunna bjóða upp á og/eða hafa komið með undanfarinn áratug, sem myndu bæta afköst kerfanna. Forritarar þurfa að vera vel vakandi fyrir nýjungum í gagnagrunnum til að skapa hugbúnaðarlausnum sínum framgang í ört vaxandi samkeppni um hraðvirkari lausnir á þeim fjölmörgu vandamálum sem glímt er við. Ég hef orðið þess áskynja í mínu fagi sem gagnagrunns- og hugbúnaðarsérfræðingur vegna aðstoðar sem ég veiti í gegnum fagvefi að kollegar hér heima og erlendis fara oft á mis við nýjungar sem í boði eru í þeim gagnagrunnum sem þeir eru að vinna á móti og eru þeir oftast þakklátir fyrir ábendingar. Lausnir þessar hafa skilað því að kerfin vinna allt að 98 prósent hraðar og og af meiri skilvirkni en þær gerðu áður.

Auðvitað skiptir val á vélbúnaði einhverju máli þar sem gagnagrunnar þurfa bæði afl og vinnsluminni. Vélbúnað þarf einnig að endurnýja reglulega og í sumum tilfellum getur það reynst nauðsyn. Val á vélbúnaði ætti þó að taka mið af því um hverskonar vinnuálag (e. workload) og gagnamagn er að ræða. Hitt er annað að rannsóknir hafa sýnt að 80 prósent af afkastavandamálum kerfa, sem nýta sér gagnagrunn, liggur í rangri kóðun á SQL fyrirspurnum miðað við þá útgáfu af gagnagrunni sem unnið er með hverju sinni. Þannig að hvort sem menn velja nýja stórtölvu, stóra, miðlungs eða litla miðlara (e. servers) þá er hagkvæmt að ráðast á þungar SQL-fyrirspurnir, töflustrúktúr og aðra gagnagrunnshögun og innleiða þær nýjungar sem í boði eru. Ein lausn sem ég lagði til á einum fagvefnum sparaði, eða öllu heldur seinkaði, kaupum erlends fyrirtækis á nýjum miðlara af miðstærð undir gagnagrunn.

Er þitt fyrirtæki magnað?

Aukið öryggi

Búrfellsvirkjun önnur er mikið mannvirki og verkfræðilegt afrek, mögulega grænasta virkjun í heimi. Þegar ÍAV fékk verkefnið þurfti að hafa hraðar hendur við að koma upp vinnuaðstöðu fjarri mannabyggðum með öruggri tengingu við höfuðstöðvar fyrirtækisins. Við hjá Opnum Kerfum höfum átt gott samstarf við ÍAV í gegnum tíðina og netlausnir okkar leystu málið. Verkinu miðar vel og frá upphafi hafa allir starfsmenn á svæðinu verið nettengdir, sem sparar tíma og fjármuni en eykur jafnframt öryggi til muna.

Allar nánari upplýsingar á www.ok.is/magnad

Opin Kerfi
– allt er mögulegt

Opin Kerfi // Höfðabakka 9 // 110 Reykjavík // 570 1000 // ok.is

Önnur ógn sem er nátengd ógninni sem lýst var hér að framan er öryggi gagnanna. Gríðarlega mikilvægt er að huga vel að því hvernig fyrirspurnir og innsending gagna og gagnabreytinga eru formaðar og prófaðar (e. validation) og sendar inní gagnagrunnana sem og hvernig gögnunum er skilað til baka til vefsins eða forritsins. Eitt þekktasta dæmið um árás á gagnagrunna er SQL-innspýting (e. SQL-injection) þar sem hakkari bætir inní SQL-fyrirspurn og eða innsláttar-textasvæði, sínum SQL-skipunum og nær þannig að komast inní gagnagrunninn. Það er alltof algengt að forritarar átti sig ekki á að nýta þá einföldu tækni sem kemur í veg fyrir slíkar árásir. SQL innspýting er í dag (árið 2017) í fyrsta sæti skv. TOP 10 lista OWASP (www.owasp.org) yfir ógnir sem steðja að tölvukerfum og gagnagrunnum.

Og því miður hafa margir stærstu gagnalekar (e. data breaches) útí heimi undanfarin ár, þar sem persónugreinanlegar upplýsingar og kreditkorta-upplýsingar hafa komist í hendur glæpagengja, einmitt notast við SQL-innspýtingu. Hjúpun SQL-fyrirspurna og innsendinga gagna í kóða, sem og notkun á gagnagrunns-stefjum (e. stored procedures) ásamt góðri og ítarlegri prófun (e. validation) gagna fyrir innsendingu, skiptir sköpum í þeirri baráttu en það vill brenna oft við að hugbúnaðarlausnir skorti slíka nálgun í hönnun. Það er sérstaklega áberandi í vefkerfum þar sem SQL kóði er berskjaldaður fyrir hökkurum og sýnilegur í vafra með því einu að opna sýn á kóða síðunnar.

LOKAORÐ

Með þróun forritunarmála og gagnagrunna skapast gríðarleg fjölbreytni í hugbúnaðarlausnum fyrir vefi, bakvinnslukerfi sem og smá-forrita. Þessari fjölbreytni ber að fagna en að sama skapi þarf að vega og meta hverju sinni með ítarlegum prófunum hvort þessi eða hin lausnin henti þeim vandamálum sem glímt er við, m.t.t. öryggis gagna og afkastagetu og eins samanburði við gömlu lausnina.

Hugbúnaðarþróun er langhlaup og eins og í langhlaupi þá krefst hugbúnaðarþróun agaðrar, vel skipulagðrar og markvissrar þjálfunar. Þjálfun og endurmenntun í hugbúnaðargerð og gagnagrunns-forritun/hönnun, í ört vaxandi tækniframförum samtímans krefst mikillar athygli hugbúnaðar-sérfræðings á þeim framförum sem verða til þess að hann/hún geti skapað sínum lausnum framgang í ört vaxandi samkeppni um betri, öruggari og hraðvirkari lausnir.

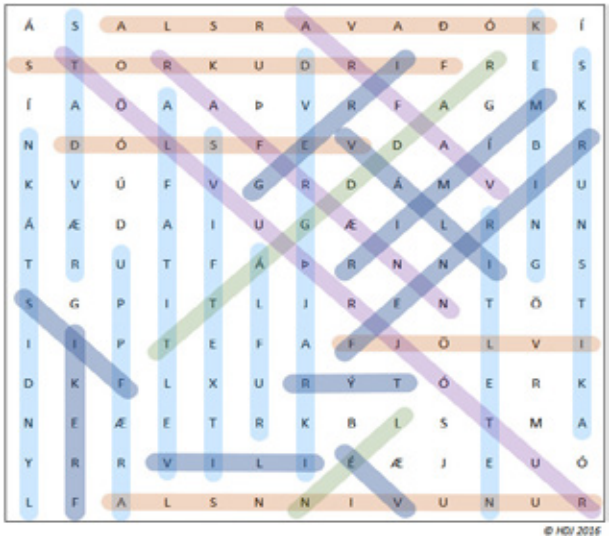
ORÐARUGL

Íslensk tölvuorð

LAUSN FRÁ SÍÐASTA BLAÐI

Í orðaruglinu var að finna íslensk heiti fyrir eftirfarandi hugtök:
Flest orðanna mátti finna á tos.sky.is, en einnig voru nokkur prufuhugtök á sveimi.

batch processing	**runuvinnsla**
browse	**vafra**
cyberstalker	**neteltir**
debugging	**kembing**
domain	**lén**
electronic	**rafrænn**
emoticon	**lyndistákn**
hacker	**tölvuþrjótur**
hint / tooltip	**sviftexti**
local	**staðvær**
macro	**fjölvi**
nanorobot	**dvergþjarki**
pivot table	**veltitafla**
refresh	**uppfæra**
scroll bar	**skrunstika**
solid-state disk	**storkudrif**
source control	**kóðavarsla**
URL	**vefslóð**
voice portal	**raddgátt**
wizard	**álfur**



Nokkrar sögupersónur úr norrænni goðafræði smeygðu sér einnig inn í gátuna:

Geri	**Vili**	**Mímir**
Freki	**Vé**	**Týr**
Fenrir	**Váli**	**Sif**

SAMSKIPTABLEKKING OG AÐRAR ÓGNIR

Daði Gunnarsson, rannsóknarlögreglumaður

Samstarf milli ólíkra aðila er afar mikilvægt til að koma á betra netöryggi. Í þessari grein mun ég fara yfir þær tilkynningar sem eru að berast lögreglu nú og hvernig við teljum best að berjast gegn þeim hættum sem eru þeim samfara, nú og í framtíð.

Það má skipta þeim sem beita netbrotum í þrjá mismunandi hópa. Fyrst er hinn hefðbundni glæpamaður, sem stundar fjársvik, fjárkúganir o.fl. í þeim dúr. Síðan þeir sem kallaðir eru hakktívistar, en það eru þeir sem brjóta af sér af einhverri hugsjón en eru ekki í brotunum til að hagnast á þeim heldur til að valda usla hjá þeim sem þeir eru á móti eða líta á sem andstæðinga sína. Að lokum eru það ríki sem eru að njósna um önnur ríki. Þær árásir eru yfirleitt mjög háþróaðar og því getur verið erfitt að berjast gegn þeim. Ég mun mest fjalla um hinn hefðbundna glæpamann, enda flestar tilkynningar til lögreglu sem snúa að þeim hópi.

Tilkynningum til lögreglu um samskiptablekkingar (e. social engineering) sem beint er gegn einstaklingum eða fyrirtækjum hefur fjölgað undanfarið. Flestir innan tölvurannsóknadeildar lögreglu þekkja dæmi um tilvik þar sem einstaklingar tilkynna ekki um brot til lögreglu vegna þess að þeir vilja ekki viðurkenna að hafa fallið fyrir slíkum blekkingum. Þetta er ekki sér íslenskt fyrirbæri, heldur vel þekkt.

Það er mjög mikilvægt að almenningur og fyrirtæki tilkynni til lögreglu ef blekkt hefur verið með þessum aðferðum, bæði til að lögregla þekki betur umfang þessara brota og ekki síður til að geta varað aðra einstaklinga og fyrirtæki við í þeim tilgangi að koma í veg fyrir frekari brot. Þeir sem stunda brotin eru yfirleitt mjög færir og má í raun tala um að þeir séu sérfræðingar í blekkingum og því ástæðulaust að skammast sín fyrir að verða fyrir barðinu á þessum einstaklingum eða hópum. Lögregla nær síður að hafa hendur í hári þeirra ef ekki er tilkynnt um brotin því tilkynningar og vitneskja um brot eru forsenda þess að lögregla geti sinnt forvörnum á þessu sviði.

SVINDL GEGNUM TÖLVUPÓST

Þekkt form samskiptablekkinga gagnvart fyrirtækjum er tölvupóstur sem sendur er á fyrirtækið. Þá er venjulega um að ræða að einhver greiðsla sem á að fara inná ákveðinn reikning endar á allt öðrum reikningi. Þetta er gert með því að senda póst á þann starfsmann sem á að greiða reikninginn og honum bent á að mistök hafi verið gerð og hann beðinn að senda greiðsluna á annan reikning. Pósturinn virðist koma frá sama fyrirtæki og á að fá greiðsluna og því áttar fólk sig ekki á þessu fyrr en of seint.

Dæmi eru um að brotin séu töluvert flóknari og þá fylgjast brotamenn meira með starfsmönnum fyrirtækja til að bæta gæði blekkinganna. Sumir eru iðnir á samfélagsmiðlum og glæpamennirnir nota þær upplýsingar til að sjá hvað fólk er að gera og hvar það er. Þannig hafa þeir jafnvel orðið áskynja um að forstjórar fyrirtækjanna eru erlendis og senda þá póst í nafni forstjórans með fyrirmælum um að breyta greiðslum eða þess háttar. Þetta eins og margar tegundir af svona brotum krefst einungis lágmarks tölvuþekkingar en snýst miklu frekar um gæði blekkinganna.

SAMSTARF OG TILKYNNINGAR

Lögreglan á Íslandi vinnur náið með erlendum lögregluliðum í baráttunni gegn netglæpum og þannig þurfa brotamenn að svara fyrir sína glæpi hvaðan sem þeir eru að fremja brotin. Það sem mögulega getur komið upp um þá er t.d. notendanöfn, tölvupóstföng, IP tölur eða hvað annað sem notast er við af glæpamönnunum.

Tilkynning til lögreglu um að einhver hafi orðið fyrir samskiptablekkingu gerir lögreglu kleyft að senda út tilkynningu til almennings um hvaða svikastarfsemi er í gangi á hverjum tíma og getur þannig jafnvel komið í veg fyrir að aðrir verði fyrir barðinu á þessum blekkingum. Lögreglan er með virka Facebook síðu sem er vinsæl meðal almennings auk þess sem fjölmiðlar fylgjast vel með og birta þaðan fréttir. Þetta teljum við mjög mikilvægt í baráttunni gegn netglæpum.

SPILLIFORRIT OG LEKAR

Það sem við sáum fyrr á þessu ári þegar tvær stórar spilliforrits (e. malware) árásir áttu sér stað, annars vegar WannaCry og hins vegar Petya eða NotPetya, er að vitundarvakning virtist verða meðal almennings. Ekki ólík þeirri vitundarvakningu sem varð með þjófnaðinum á notendaupplýsingum frá Ashley Madison. Í Ashley Madison lekanum má segja að fólk sem var ekki mikið að spá í netöryggi hafi áttað sig á því að þær upplýsingar sem það skráir á netinu geta lekið út. Sumsé áttað sig á því að fara varlega með hvaða upplýsingar það skráir.

Þessar tvær spilliforrits árásir þar sem spítalar í Bretlandi og eitt stærsta skipaflutnings¬fyrirtæki í heiminum, Maersk, urðu illa úti var fjallað ítarlega um það í fjölmiðlum og fólk varð meðvitaðra um þessa hættu. Þetta er mikilvægt því það næst ekki árangur fyrr en sem flestir þekkja til þessara brota og verða skilja mikilvægi netöryggis.

Lögregla hefur fengið tilkynningar um svona gíslatökuforrit hér á Íslandi, þó að NotPetya hafi ekki verið eiginlegt gíslatökuforrit, og hafa einstaklingar og fyrirtæki orðið fyrir barðinu á slíkum óværum. Í þeim málum má segja að fólk hafi lært að taka reglulega öryggisafrit af gögnum sínum þannig að skaðinn af svona árás verði sem minnstur.

KÚGANIR OG SVIK GEGNUM NETIÐ

Lögreglu hafa borist tilkynningar um að einstaklingar hafi verið að kynnast öðrum einstaklingum gegnum netið á rómantískan eða kynferðislegan hátt. Tilkynningarnar sem við höfum verið að fá einnig þær að einstaklingur sem býr erlendis en vill endilega koma til landsins og heimsækja brotaþolann. Viðkomandi einstakling vantar aftur á móti pening til þess að geta komið í heimsókn til brotaþolans og fær brotaþolann til að leggja

inn á sig pening. Svona svik eru vel þekkt og nánast eina leiðin til að berjast gegn svona er að tilkynna fólki um þessa hættu í samskiptum við ókunnuga, þ.e. að fólk sé meðvitað um þess konar brot.

Þá hafa einnig borist tilkynningar um að einstaklingar hafi verið í einhverjum kynferðislegum athöfnum á netinu og ekki gert sér grein fyrir því að hinn aðilinn er að taka upp og eftir á fer handhafi upptökunnar að kúga hinn um fé. Það er sama með þessi brot. Við berjumst gegn þessu með vitundarvakningu og upplýsum fólk um þessi brot.

Sú flóra af tilkynningum sem lögreglan er að fá sýnir að flestar tegundir brotanna eru ekki endilega tæknilega flóknar. Stór hluti þeirra byggist á blekkingum en ekki innbroti í tölvukerfi eða sérfræðiþekkingu á tölvum.

SÍMASVINDL

Þá eru að berast tilkynningar um símhringingar frá erlendum númerum til fólks sem það nær ekki að svara. Fólk hringir til baka en áttar sig ekki á því að númerið er gjaldskylt og það situr uppi með reikninginn. Almennt er fólk ekki að tapa stórum upphæðum en ef margir hringja í þessi númer þá er upphæðin sem brotamaðurinn fær í hendur umtalsverð.

Einnig hafa borist tilkynningar um öllu tæknilegri brot. Þá er brotist inná IP símkerfi og þegar vinna liggur niðri hjá því fyrirtæki sem á eða er með símkerfið þá er hringt erlendis í gjaldskyld númer sem brotamennirnir eiga og getur svona brot þess vegna staðið dögum saman, t.d. ef fyrirtækið er lokað um helgar.

FRAMTÍÐIN

Við höfum séð að með svokölluðum IoT (e. Internet of Things) þá eru margir framleiðendur sem hafa ekki verið að hugsa um netöryggi. Á síðasta ári sáum við tvær stórar DDoS árásir framkvæmdar með hinu svokallaða Mirai yrkjaneti (e. botnet). Þar sem netöryggi var ekki haft að leiðarljósi við gerð margs búnaðar þá var hann einfaldlega opinn fyrir því að vera sýktur og notaður í svona árásir. Þegar fólk er meðvitað um þessa hættu bregst það vonandi við henni, þ.e. kemur sér upp vörnum þannig að búnaðurinn sé ekki opinn fyrir árásum.

Lögreglan vill og þarf að vera í nánu sambandi við almenning og fyrirtæki landsins til að geta upplýst um glæpi og helst komið í veg fyrir að hægt sé að fremja þá. Það verður hægt að hluta til með aukinni vitundarvakningu sem fæst með samhentu átaki allra aðila og að öll brot séu tilkynnt til lögreglu, þannig að í það minnsta sé til vitneskja að brot hafi átt sér stað.

Hægt er að senda tölvupóst með tilkynningum um netglæpi og aðrar fyrirspurnir á: dadi.gunnarsson@lrh.is eða cybercrime@lrh.is

BEBRAS ÁSKORUN 2017

FER FRAM Í SKÓLUM LANDSINS VIKUNA 6. - 10. NÓVEMBER 2017 OG ER OPIN ÖLLUM SKÓLUM MEÐ NEMENDUR Á ALDRINUM 8 - 18 ÁRA

Bebras áskorunin er alþjóðlegt verkefni (e. International Challenge on Informatics and Computational Thinking) sem felst í því að nemendur nota rökhugsun og tölvufærni til að leysa skemmtilegar þrautir byggðar á hugsunarhætti forritunar. Bebras er haldið árlega á sama tíma í um 50 löndum um allan heim og er Ský í forsvari fyrir verkefnið á Íslandi.

Þrautirnar eru hugsaðar fyrir 8 - 18 ára aldur og skipt niður eftir aldri. Bebras áskorunin er eitt fjölmennasta verkefni sem notað er til kennslu í upplýsingatækni. Hún var haldin í fyrsta sinn á Íslandi í nóvember 2015 og þá tóku tæplega 500 nemendur frá 14 skólum þátt í áskoruninni. Árið 2016 voru tæplega 2.000 nemendur með frá 18 skólum og í ár er stefnt á að fá enn fleiri skóla með.

HVAÐ ER BEBRAS?

Bebras var upphaflega stofnað af Prófessor Valentina Dagiene hjá Háskólanum í Vilnius, en Bebras (e. Beaver) er litháíska heitið á dýrinu bifur. Hún ákvað að nýta bifur sem ímynd áskorunarinnar vegna þess dugnaðar og fullkomnunaráráttu sem þeir virðast hafa. Bifur er duglegt, vinnusamt og gáfað dýr sem vinnur stöðugt í stíflunum sínum til að gera þær betri og stærri. Fyrsta Bebras áskorunin var í Litháen árið 2004 og hefur vaxið gríðarlega á stuttum tíma og nú er Bebras eitt fjölmennasta verkefni í heiminum sem hefur það að markmiði að auka áhuga krakka á upplýsingatækni.

Nánari upplýsingar um Bebras má finna á www.bebras.is

SKEMA
Í HÁSKÓLANUM Í REYKJAVÍK

HELGARNÁMSKEIÐ SKEMA
fyrir 4-16 ára

SKAPANDI TÆKNI MEÐ SKEMA Í HR

Námskeiðin byggja á Skema-aðferðafræðinni sem er studd af rannsóknum á sviði sálfræði, kennslufræði og tölvunarfræði.

Flestir grunnskólar landsins meta námskeið hjá Skema til valeininga.

21.-22. OKTÓBER 2017

09:00 - 13:00 MINECRAFT og Videógerð 10 - 14 ára	14:00 - 17:00 KANO TÖLVAN & Forritun 8 - 12 ára

28.-29. OKTÓBER 2017

09:00 - 13:00 UNITY3D Tölvuleikjaforritun 11 - 16 ára	14:00 - 17:00 Tækjaforritun 7 - 10 ára

4.-5. NÓVEMBER 2017

09:00 - 13:00 MAYA 3D hönnun & hreyfimyndagerð 11 - 16 ára	14:00 - 17:00 MINECRAFT Vísindi og Herkænska 8 - 12 ára

2.-3. DESEMBER 2017

09:00 - 12:00 TÆKNISTELPUR 7 - 10 ára	13:00 - 16:00 TÆKNISTELPUR 10 - 13 ára

NÁNARI UPPLÝSINGAR OG SKRÁNING

>>skema.is / 599_6200 / skema@ru.is /

skemasetrid
SkemaEducation
Skema_Education

VEIKASTI HLEKKURINN

Þorvaldur Henningsson og Björn Ingi Victorsson,
áhætturáðgjöf Deloittes

Þrátt fyrir að fyrirtæki hafi undanfarin ár varið auknum fjármunum í kaup á búnaði til að verja upplýsingakerfi sín hefur árangursríkum netárásum samt fjölgað. Hvað veldur og hvað er til ráða?

Vissulega er mikilvægt að tryggja að upplýsingakerfi séu með skilvirkum netvörnum en ýmislegt bendir til þess að fyrirtæki verði áfram berskjölduð gagnvart netárásum ef þau leggja ekki aukna áherslu á að þjálfa starfsmenn í umgengni við internetið.

Ein algengasta brotaleiðin hjá tölvuglæpamönnum í dag eru vefveiðar (e. phishing) þar sem sendandi tölvupósts villir á sér heimildir og sendir tölvupósta með það að markmiði að blekkja viðtakanda til að gefa upplýsingar svo sem lykilorð og/eða að smella á viðhengi sem hefur að geyma tölvuvírus.

Tölvuglæpamenn virðast í auknum mæli átta sig á því að við mannfólkið erum veikasti hlekkurinn í netvörnum. Þeim hefur reynst tiltölulega auðvelt að plata móttakendur veiðipósta til að smella á viðhengi og hlaða þannig óafvitandi niður tölvuvírus. Því er þetta oft á tíðum fljótleg, ódýr og mikið notuð leið til að dreifa árásarbúnaði í tölvur.

Oft er um markvissar árásir að ræða þar sem tölvupóstar eru útbúnir til að líta út eins og þeir komi frá trúverðugum sendanda, til dæmis framkvæmdastjóra eða yfirmanni tölvumála. Tölvubúnaður sem hefur verið sýktur á þennan hátt getur gefið árásaraðila margar leiðir til að brjóta á fórnarlambi sínu, t.d með gagnagíslatöku (e. ransomware attack), hlerunum (e. surveillance software) eða hreinlega fullri stjórn yfir sýktri tölvu. Allt þetta og meira til geta þeir gert án þess að fórnarlambið taki eftir því, en rannsóknir hafa sýnt að mörg fyrirtæki eru ekki nægilega góð í að átta sig á því að tölvur hjá þeim eru sýktar vírusum.

ÁRANGURSRÍKAR VEIÐAR

Hluti af ástæðu þess að vefveiðar eru jafn árangursríkar og raun ber vitni er að fjöldi tölvupósta sem notendum berst á degi hverjum er slíkur að erfitt getur reynst að vera á varðbergi gagnvart veiðipóstum. Það eykur svo enn á hættuna að tölvuglæpamenn eru úrræðagóðir þegar kemur að því að blekkja viðtakendur og smjúga framhjá ruslpóstsíum.

Stóraukin notkun fólks á samfélagsmiðlum hefur einnig hjálpað glæpamönnum að nálgast meiri og persónulegri upplýsingar um einstaklinga sem þeir geta notað til að sérsníða efni tölvupósts á þann veg að líklegt sé að það höfði til viðtakanda.

Veiðipóstur sem virðist oftast ná tilætluðum árangri líkist að efninu til pósti sem starfsfólk fær reglulega í starfi sínu. Tölvuglæpamaður getur til dæmis sent veiðipóst til starfsmannastjóra fyrirtækis þar sem vírussmitað kynningarbréf eða starfsferilsskrá eru í viðhengi. Opni starfsmannastjórinn slíka skrá, er tölva hans sýkt og mögulega hefur tölvuglæpamaðurinn þá aðgang að öllum gögnum sem starfsmannastjórinn hefur aðgang að hjá fyrirtækinu.

HVERNIG GETUM VIÐ GREINT VEIÐIPÓSTA?

Samkvæmt reynslu netöryggissérfræðinga Deloitte, sem m.a. framkvæma veiðipóstaprófanir fyrir fyrirtæki, er algengt að u.þ.b. 30% viðtakenda veiðipósta falli í gildruna sem fyrir þá er lögð. Hafa ber í huga að oftast dugar að einn starfsmaður falli fyrir veiðipóstinum til að tölvuglæpamaðurinn geti byrjað að athafna sig í tölvukerfi fyrirtækis.

Árangur veiðipóstaprófana bendir til þess að starfsmenn séu í sumum tilfellum einfaldlega ekki nægilega vel á varðbergi þegar kemur að meðhöndlun tölvupósts. Önnur skýring er að starfsmönnum getur reynst erfitt að greina og meðhöndla veiðipósta. Þetta er sterk vísbending um að skortur sé á þjálfun og fræðslu um skaðsemi veiðipósta og hvernig greina megi slíkan póst frá öðrum tölvupósti. Mikilvægi þess að fyrirtæki þjálfi starfsmenn sína í meðferð internetsins er síst minni en mikilvægi annarra hefðbundinna netvarna. Þegar kemur að slíkri þjálfun er að mörgu að huga og mikilvægt er að vandað sé til verka.

GÖGN TEKIN Í GÍSLINGU

Nýlegar rannsóknarniðurstöður benda til þess að algengast sé að markmiðið með veiðipóstum sé að dreifa einhvers konar gagnagíslatökubúnaði. Skemmst er að minnast WannaCry gagnagíslatöku-árásarinnar, þar sem hundruð þúsunda tölva sýktust af vírus.

Gagnagíslatökubúnaður er tegund spilliforrita sem nýtt eru til að kúga fjármuni af fórnarlömbum. Slík árás getur haft víðtæk áhrif á fyrirtæki og stofnanir af öllum stærðum og gerðum. Óprúttnir aðilar geta notað slíkan búnað til að taka gögn í gíslingu með því að dulkóða þau á þann veg að eigandi gagnanna kemst ekki í þau nema hann fái dulkóðunarlykil í formi lykilorðs til að afkóða þau.

ÓGNIN MAGNAST

Samkvæmt niðurstöðum rannsókna sem nýverið hafa verið birtar hefur mikil þróun átt sér stað í gagnagíslatökubúnaði, sem hefur gert hann skeinuhættari en áður. Þannig kemur fram í skýrslu ENISA (European Network and Information Security Agency) frá janúar 2017, að árásirnar séu:

- Markvissar og valdi þannig skemmdum á öryggisafritum, gagnagrunnum, vefsíðum o.fl.
- Með öflugri dulkóðun og betri tækni til að komast hjá því að tilraun til sýkingar sé uppgötvuð.
- Með eiginleika til að hækka lausnargjald ef notendur greiða ekki innan gefins frests.
- Komnar með enn betri aðferðir til að eyða gögnum ef ekki er greitt fyrir lokafrest.
- Studdar af háu þjónustustigi til að veita fórnarlömbum tæknilega aðstoð við greiðslu lausnargjalds, t.d. með því að nota spjallrásir og í sumum tilfellum símaþjónustu við að leiðbeina hvernig hægt sé að greiða gjald með rafrænum gjaldmiðli, s.s. Bitcoin.

Á AÐ GREIÐA LAUSNARGJALDIÐ?

Það er ljóst að gerendur eru oftast að sækjast eftir skjótfengnum gróða. Því meira sem þeir græða, þeim mun líklegra er að þeir haldi áfram iðju sinni og jafnvel að fleiri stökkvi á vagninn. Því getur verið best að skoða fyrst hvort einhverjar aðrar leiðir séu í boði til að endurheimta gögnin á ódulkóðuðu formi án þess að greiða tölvuglæpamönnunum lausnargjald. Þjónustuaðilar geta oft hjálpað til við að bjarga málum. Einnig er vert að

benda á vefsíðuna nomoreransom.org, sem er samstarfsverkefni ýmissa löggæslustofnana víða um heim, s.s. Europol og fyrirtækja í tækniiðnaðinum. Á vefsíðunni er að finna fróðleik um gagnagíslatökubúnað en einnig eru þar tól til að losa gögn úr gíslingu ýmissa afbrigða af gagnagíslatökubúnaði.

Hafa ber í huga að það að borga lausnargjald þarf ekki endilega að hafa í för með sér að gögnin endurheimtist. Í sumum tilfellum hafa þeir sem greitt hafa lausnargjald ekki fengið gögnin sín á nýjan leik.

HVAÐ ER TIL RÁÐA?

Fyrirtæki þurfa vissulega að gæta þess að tækniinnviðir lágmarki hættuna á því að veiðipóstar og annar ruslpóstur berist starfsmönnum. Það eitt og sér dugar þó ekki, því gæði veiðipósta hafa aukist og vel gerðir póstar geta sloppið í gegnum slíkar síur.

Vírusvarnir þurfa að sjálfsögðu að vera til staðar og uppfærðar. Nýir vírusar líta dagsins ljós á hverjum degi þannig að hættan er samt til staðar. Auðvitað þarf að gæta að afritatöku gagna og uppfærslum á hugbúnaði til að lágmarka hættuna á að í upplýsingakerfi fyrirtækisins séu þekktir veikleikar, svo sem veikleikar í gamalli útgáfu af stýrikerfi.

Lengi mætti halda áfram að telja upp ýmis tæki og tól sem nauðsynleg eru í netvörnum og öruggum rekstri upplýsingakerfa. Þó að fyrirtæki sé með alla tækniinnviði eins og best verður á kosið er hættan samt sem áður til staðar, því vefveiðar eru nýttar til að ráðast á veikasta hlekkinn í tölvuöryggi, þ. e. okkur mannfólkið. Því er mikilvægt að fyrirtæki og stofnanir fræði starfsfólk um hætturnar, hvernig á að koma auga á þær og hvernig á að varast þær.Mikilvægt er að vandað sé til verka við upplýsingagjöf um hættur sem að okkur steðja á internetinu því dæmin sanna að afleiðingar innbrota í tölvukerfi fyrirtækja geta verið mjög alvarlegar.

GETUM VIÐ GERT OKKUR SJÁLF GREINDARI?

Arnar Jóhannsson, nemandi við Háskólann í Reykjavík

Tæknin er stór partur af lífi okkar í dag og mun vera það í framtíðinni. Tækninni fer sífellt fram og ný tækni lítur dagsins ljós á hverjum degi. Það er kostir og gallar við alla þessa tækni en hún er óumflýjanleg. Fólk hefur verið að þróa aðferðir sem gera tölvum kleift að skynja og skilja umhverfið sitt og taka rökréttar ákvarðanir í sambandi við það. Gervigreind í dag er kannski ekki komið eins langt og sumar kvikmyndir láta í veðri vaka, en hún er út um allt í kringum okkur þótt við tökum kannski ekki eftir því.

Í gervigreind er gjarnan notast við tauganet (e. neural network) þar sem vélin kennir sér sjálf og lærir af mistökum og er það helst notaða gervigreindar reikniritið í dag. Þekkingarkerfi (e. rule based systems) eru einnig notuð í gervigreind og er þá forritað frá grunni þar sem forritari skráir sjálfur inn þær reglur sem vélin á að nota og þekkja.

Watson er nafn á tölvu sem var þróuð af fyrirtækinu IBM. Tölvan notar tauganet til að læra en er einnig með ákveðið þekkingarkerfi sem hún notar við reikninga og staðreyndir. Þekkingarkerfi Watson er því sífellt að stækka og verður greindari með hverjum deginum. Í fyrstu var Watson bara tölva sem vann bestu taflspilara í tafli en var síðan þróuð í að vinna allra bestu spilara í Jeopardy! Watson sigraði í Jeopardy! í viðureign gegn fyrrum sigurvegurum, Brad Rutter og Ken Jennings, fyrir um sex árum og hefur síðan verið í stöðugri þróun.

Við manneskjurnar erum svipuð og Watson, lærum grunnupplýsingar á okkar fyrstu 18 árum og eftir það sérhæfum við okkur í einhverju sviði. Watson er einmitt að sérhæfa sig á ákveðnu sviði, hann er að hjálpa heilbrigðisþjónustunni við að greina sjúklinga og fara yfir ýmsar læknisritgerðir til að finna lausn á flóknum vandamálum.

En hvað ef Watson hefði annan tilgang? Hvað ef hann gæti búið til aðra tölvu greindari en sig? Hvað ef sú tölva myndi síðan gera aðra tölvu snjallari en sig og hún myndi gera það sama þar til við myndum enda á hafa tæknisprengju (e. Intelligence explosion). Framúrskarandi tækni (e. technological singularity) er hugtak yfir þróun tækninnar og þann tímapunkt í sögunni þegar gervigreind (e. artificial intelligence) endar með að vera greindari en maðurinn. Þá myndu greind vélmenni taka yfir heiminum. Í gamla daga var þetta einungis kenning sem John Von Neumann birti árið 1950. Nú eru menn farnir að halda að þetta gæti gerst og sumir vilja reyna að koma í veg fyrir þetta. Elon Musk, forstjóri Tesla og SpaceX, er virkilega að spá í spilin og hefur fjárfest í mörgum fyrirtækjum sem eru að vinna að þróun gervigreindar, til að fylgjast vel með þróuninni sjálfur.

Margir rithöfundar hafa skrifað bækur um hvernig lífið væri ef „Singularity“ myndi gerast en meðal þeirra frægustu eru „The Singularity is Near“ eftir Ray Kurzweil og „Singularity Sky“, skáldsaga eftir Charles Stross. Sú fyrri fjallar um spár Kurzweil um framtíðina og hvernig tölvur munu hafa tekið yfir heiminn um árið 2045. „Singularity Sky“ fjallar um lífið eftir að vélar hafa tekið yfir heiminn (e. post-singularity) og fékk Charles Stross hin virtu Hugo verðlaunin fyrir bókina.

En hvað ef í stað þess að gera vélmenni sem eru snjallari en við þá gerum við okkur sjálf greindari? Maður að nafni Bryan Johnson stofnaði fyrirtækið Braintree árið 2007 og seldi það sex árum seinna til eBay fyrir 800 milljón dollara. Bryan notaði 100 miljónir af þeim peningum til að byrja nýtt fyrirtæki að nafni Kernel. Kernel er að skoða möguleikann á því að tengja ígræðanleg tæki (e. implantable device) við heila mannsins. Slík tæki myndu vera geymsla á minni sem hægt væri að nota sem vitneskja manneskjunnar. Einnig á tækið að tengjast við gervigreind sem gæti gert einstaklingnum lífið létt. Gervigreindin myndi sjá um alla stærðfræði útreikninga og vinnslu á meðan heilinn þyrfti bara að sjá um tilfinningar og list. Rannsóknir á taugakerfinu (e. neuroscience) eru samt ekki komnar nógu langt að við getum almennilega vitað hvað er að gerast í heilanum.

Ýmis fyrirtæki eru að vinna á þessu sviði þar á meðal Neuralink þar sem Elon Musk er forstjóri. Ef þessi verkefni takast þá værum við ekki bara að þróa gervigreindina heldur væri um að ræða þróun mannkynsgreindar (e. human intelligence).

HEIMILDIR:

https://en.wikipedia.org/wiki/Bryan_Johnson_(entrepreneur) https://www.inverse.com/article/13630-what-has-ibm-watson-been-up-to-since-winning-jeopardy-5-years-ago https://en.wikipedia.org/wiki/Watson_(computer) https://en.wikipedia.org/wiki/Technological_singularity
https://www.visindavefur.is/svar.php?id=264

RISKS OF THE INTERNET OF THINGS

Marcel Kyas, lector Háskólanum í Reykjavík

The Internet of Things (IoT) is easiest described as a network of physical objects that are addressable on the internet through an internet protocol (IP) address. They communication with other Internet-enabled devices and systems.

IoT is seen as a trillion-dollar business. From a current estimate of 15.4 billion devices, IHS Markit forecasts that the market will grow to 30.7 billion devices in 2020 and 75.4 billion devices in 2025. Annual revenues are expected to exceed $470 billion by 2020, according to Bain.

IoT devices are used in industry, logistics, and daily life. Many manufacturing plants use Ethernet and IP addressing to reduce cost and simplify construction of the plats. Such a communication architecture is even used in the Airbus A380. As long as the environment of such systems is controlled, manufacturers can reduce cost and improve the performance of inter-device communication.

In uncontrolled environments, especially where the devices are exposed to the internet, security of IoT devices becomes a priority.

The features provided by those devices can be considered useful to many people. By choosing Internet technology to have devices communicate among each other and with providers of external processing, the devices are accessible from the Internet and thus may be susceptible to attacks from the Internet. Anyone that knows the IP address and the service provided by the devices connected to the internet can connect to the device and use its service.

THINGS

Before I describe the security implications, I give examples of things: Philips Hue Smart Bulbs can change colour and be switched on and off. They can be connected to home hubs and controlled from smart phone applications. Sport activity trackers communicate with smart phones, which in turn provide a bridge to the internet. Smart power plugs monitor the power use at the plug and allow connected devices to be switched on and off. The promise is that by monitoring the energy use, home owners can make their homes more energy efficient. Smart thermostats allow to monitor the power use of heating systems and to adapt the ambient temperature to the persons present. Smart locks promise to dispose of keys and fobs, controlling all locks through a smart phone.

Smart security systems can monitor houses through (night-vision) cameras, microphones, motion detectors. If the system detects something worthwhile, it will communicate with its owner and stream video or audio to one of his devices.

Smart TVs use microphones and cameras to interact with its users, enabling them to communicate with other people, e.g., through Skype, or to control the device with voice commands or gestures.

The Shodan project (http://shodan.io/) provides a search engine for internet connected devices.

ATTACKS

What interest do assailants have in IoT devices?

While those devices may just look like normal devices, they usually contain a low-powered computer and they have an Internet connection. Often the computational capabilities are sufficient for parasitic computing tasks. They can be used as part of distributed denial of service attacks, to distribute SPAM, or to mine crypto currencies.

While each individual device may not be powerful, they are mass produced devices and in their number, they are a formidable platform. The Mirai bot net was used on October 21 to disrupt internet activity in the US by attacking the Domain Name Service. The bot-net consisted of about 100.000 nodes.

Such attacks are possible, because capturing and controlling such devices can be mechanized easily. The devices are mass-manufactured and delivered with identical software and configuration. Buyers often feel challenged and ill-informed in changing the configuration.

Other attacks involve invasions of privacy. Smart TVs, for instance, are constantly listening for their command word. An attacker controlling that device can eavesdrop on any conversation inside the room the TV is in. Attackers can also capture web cameras and capture video and audio recordings from such rooms.

Unsecured web cameras are known to be used to capture bedroom activities. Such recordings can be monetized or sold or displayed on web pages for advertisement impressions.

Devices can also be taken ransom. Shutting down a thermostat in winter and demanding ransom can put people in life-and-death situations.

FAILURES

Also, failures of the infrastructure can cause harm to people. Many IoT devices rely on services provided by other machines on the internet. Voice and image processing can be difficult, and it is considered cheaper to record a command, send it to a more powerful server for processing, and sending a command back to the device. This way, the cost for each individual device can be kept down and the processing power can be utilized better.

But what happens if the server fails? If a TV does not react to a command, it is inconvenient. A door that cannot be opened by its smart phone application may be a much bigger problem. Some car doors can only be operated this way in the presence of mobile phone networks. Driving into areas without one, like Iceland's high lands, may lock you out or in your car.

In other cases, thermostats shut down because their cloud service was not available and in some instances, houses were taken of the electric grid for the same reason.

DESIGN IMPLICATIONS

The nature of the attacks on IoT devices and the failure modes require stringent engineering methods that most companies are not used to yet.

Governments and consumer associations demand improved security mechanisms and processes. They wish that security issues that show up after manufacturing get corrected by firmware updates for an extended time. Some even demand certified code, development processes, and security management processes, on the server side and also on devices.

Those mechanisms concern passive security. The system is hardened against attackers. A second, complementary approach is to help users secure their devices by forcing them to change access codes and to correctly configure their firewalls. Some suggest that the internet providers should help users with tracking and securing the internet connections.

The third mechanism is to make fail-safe designs. The software on the thing must deal gracefully if part of the infrastructure it relies on is not available. A thermostat should not shut down heating if the cloud service is not available. Instead, it should choose a safe default temperature, say 25 degree centigrade. A lock may default to an unlocked state in the same situation.

---

eIDAS: UPPRUNI TRAUSTS

Elfur Logadóttir, lögfræðingur, framkvæmdastjóri ERA

Við höfum öll séð hvað tækninni hefur undið fram; hvernig tækninýjungin hver á fætur annarri hefur gert líf okkar auðveldara og þægilegra en á köflum flóknara. Við sjáum tæknilausnirnar stíga inn á öll svið mannlífsins, hvort sem það er í heilbrigðisgeiranum eða á hárgreiðslustofunni, tölvan og annar tæknibúnaður hefur aðkomu að einföldustu ferlum. Á sama tíma sjáum við hvernig hætturnar – ógnirnar – sem af tölvutækninni stafa, lúra handan við hornið og nýta sér hvert tækifæri sem gefst, hvern þann veikleika sem finnst – eða, þannig hefur fræðslan verið undanfarinn áratug.

Við höfum endurtekið heyrt skilaboðin um að tækninni fylgi veikleikar – að hún sé óörugg; að henni verði ekki treyst. Okkur hefur verið sagt að gera ráð fyrir því að tölvan okkar sé sýkt með einhverjum hætti, að við höfum ekki fulla stjórn á henni í reynd og jafnvel að ganga svo langt að gera ráð fyrir því að allt sem við gerum með tækninni sé á allra vitorði. „Treystu engum, skrifaðu tölvupóstana eins og þeir væru póstkort sem allir geta lesið, því þeir eru það". Þannig hefur því sífellt verið haldið að samfélaginu að tækninni sé ekki treystandi.

SAMHENGI HLUTANNA

Um þessar mundir eru 10 ár síðan ég skrifaði tvær meistaraprófsritgerðir á sviði persónuverndar sem báðar fjölluðu um ógnina sem persónuvernd stafar af tækninni; önnur tæklaði örmerkingar (RFID) og hvernig viðleitni framleiðenda til þess að ná niður framleiðslukostnaði örmerkja leiddi til þess að þau voru strípuð af öllu öryggi og veittu þar með enga vernd fyrir persónuna sem bar þau; hin ritgerðin fjallaði um umferðagögn í fjarskiptum og þær persónuupplýsingar sem til verða á ýmsum stöðum við notkun fjarskiptatækja, hvort sem er farsíma eða annarra nettengdra tækja. Báðar voru ritgerðirnar skrifaðar í árdaga allrar umræðu um gögn og verðmæti þeirra upplýsinga sem markviss söfnun hegðunar- og umferðargagna færir safnaranum og hvorug þeirra þorði að sjá fyrir þá geigvænlegu söfnun sem raunveruleg er orðin, þó höfundurinn hafi af mörgum verið talin þokkalega „nojuð" í rannsóknarvinnunni.

En hvers vegna að nefna þetta núna, þegar við erum öll orðin vön því og höfum fyrir löngu sætt okkur við alla þessa söfnun upplýsinga sem nútímasamfélagið ber með sér? Það er vegna þess að eitt svið mannlífsins hefur verið margfalt íhaldssamara en önnur og þrjóskast við tækniþróuninni: Lögfræðin.

INNBYGGÐ ÁHÆTTUSTÝRING

Það er lítið mál að kaupa sér bækur, varahluti, tæknibúnað og flestar nytjavörur á netinu – jafnvel frá fjarlægum stöðum í heiminum – en þegar kemur að stærri löggerningum með lengri og varanlegri áhrifum þá hefur innbyggð áhættustýring lögfræðinga sagt stopp. Fasteignir eru ekki seldar rafrænt; þinglýsingar, þó þær séu unnar og skráðar rafrænt, þá byggja þær að öllu leyti á því að til sé frumrit á pappír; fullnusta löggerninga (aðför, nauðungarsala, og þess háttar) krefst þess að löggerningarnir hafi verið skráðir á pappír; kaupmálar, erfðaskrár, forsjársamkomulag og aðrir samningar sifjaréttarins verða eingöngu gerðir á pappír; og íslenskir dómstólar gera almennt ráð fyrir því að hugtakið skjal nái ekki til rafrænna gagna.

Og ástæðan er einföld: **Takmarkað traust.**

Lögfræðinga skortir það traust á tæknina sem nauðsynlegt er til þess að unnt sé að flytja þessar tegundir löggerninga yfir á rafrænt form eingöngu. Reynslan hefur kennt þeim að þegar allt annað þrýtur, þá hefur vel varðveittur löggerningur, prentaður á pappír sem viðheldur gæðum sínum í hundrað ef ekki hundruð ára og geymdur í eldvörðum skápum eða bankahólfum, tryggt einstaklingum fullnægjandi réttarvernd í árhundruð. Í hvert sinn sem tæknivæðingu ber á góma standa upp lögfræðingarnir sem reynslu og þekkingu hafa á landamerkjadeilum fortíðarinnar og minna á aldagamla pappírinn sem réði úrslitum í þessu eða hinu málinu. Það verður að tryggja varanlegan aðgang að skjölum sem varðað geta hagsmuni í framtíðinni.

Verkefnið er þess vegna að bæta traust lögfræðinga á rafræn ferli, að þau haldi og að þau geti verið sett fram með nægjanlega varanlegum hætti hverju sinni, misvaranlegum eftir efni, tilgangi og gildistíma löggerninga.

eIDAS, REGLUGERÐ EVRÓPUSAMBANDSINS

Það var í þessum tilgangi sem Evrópusambandið réðst í ritun nýrra reglna til þess að koma í stað 15 ára gamals regluverks sem átti að tryggja nægjanlega lagaumgjörð fyrir upplýsingasamfélagið eins og það var kallað. eIDAS, reglugerð ESB um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum var staðfest í júlí 2014 og tók

gildi í ESB ríkjum að mestu leyti þann 1. júlí 2016. Síðasti hluti reglugerðarinnar, sá sem lýtur að rafrænni auðkenningu, mun taka gildi í september 2018 og verður reglugerðin þá að fullu innleidd í Evrópusambandinu.

Með eIDAS reglugerðinni er ætlunin að byggja upp traust á rafrænni þjónustu á innri markaði Evrópska efnahagssvæðisins – sameiginlegan rafrænan innri markað – með því að skilgreina samræmdar, tæknilegar og ferlatengdar kröfur og gæðin að baki þeim þjónustuþáttum sem nýttir eru í rafrænum viðskiptum. Hugtakið traustþjónusta er þannig notað um tiltekna tæknilega þjónustuþætti sem auka öryggi og lögmæti rafrænna samskipta. Kröfur til rafrænnar auðkenningar eru jafnframt staðlaðar til að tryggja samræmdan skilning og samræmda notkun á öllu evrópska efnahagssvæðinu.

TRAUSTÞJÓNUSTA, NÝTT HUGTAK

Til traustþjónustu skv. eIDAS reglugerðinni teljast sjö mismunandi þættir:

1. Myndun **rafrænnar undirskriftar**, þ.e. sú aðgerð að einstaklingur staðfesti með rafrænum hætti ásetning sinn til þess að vera skuldbundinn af efni þess gernings sem þannig er undirritaður. Undirritun getur jafnframt verið framkvæmd af einstaklingi í bærni hans til þess að skuldbinda lögaðila.
2. Myndun **rafræns innsiglis**, þ.e. sú aðgerð að lögaðili staðfesti heilleika og uppruna þess gernings sem þannig er innsiglaður. Hér getur ýmist verið um að ræða sjálfvirka aðgerð kerfis sem byggir á skilgreindu ferli sem samþykkt hefur verið af einstaklingi með bærni, eða að einstaklingur sem er þar til bær, staðfesti fyrir hönd lögaðila umræddan gerning.
3. Myndun **tímastimplunar**, þ.e. sú aðgerð ytri aðila að veita staðfestingu á tímasetningu aðgerðar. Tímastimplun er jafnan nýtt til að staðfesta tilvist rafræns skjals á tilgreindum tíma.
4. **Rekjanleg rafræn afhendingarþjónusta**, þ.e. sú aðgerð að afhenda rafræn skjöl og aðrar rafrænar afurðir með traustum rekjanlegum hætti frá einum aðila til annars.
5. **Sannvottun vefsetra**, þ.e. traustar upplýsingar á vefsíðu (vottorð) sem gerir notendum kleift að staðfesta réttleika vefsíðunnar og tengsl hennar við aðilann sem stjórnar henni.
6. **Sannprófun og staðfesting** rafrænna undirskrifta, rafrænna innsigla, rafrænna tímastimpla, rekjanlegrar rafrænnar afhendingarþjónustu og vottorða sem tengjast þessum þjónustum ásamt vottorðum sem tengjast sannvottun vefsetra.
7. **Varðveisla** á rafrænum undirskriftum og innsiglum eða vottorðum tengdum þessum þjónustum.

Því til viðbótar setur reglugerðin fram meginreglu um bann við mismunun skjala og aðgerða af þeirri ástæðu einni að skjölin eða aðgerðirnar eru á rafrænu formi auk þess að tryggja viðurkenningu á rafrænni auðkenningu og traustþjónustum yfir landamæri.

Það er mat ESB að með reglugerðinni megi tryggja nægilegt samræmi í vöruframboði og vöruþróun traustþjónustu í einstökum aðildarríkjum að nú verði loks unnt að treysta aðilum á milli landa og að á verði komið skilvirkum rafrænum innri markaði á EES svæðinu. Að sameiginlega eigi efniskaflar reglugerðarinnar að mynda rammann utan um fullnægjandi traust til tækninnar til þess að ljúka megi hvaða ferli sem er með rafrænum hætti; fara alla leið.

Á HVERJU BYGGIR TRAUSTIÐ?

Það er lengra og flóknara að skýra en kemst fyrir í grein sem þessari en í grunninn byggir traustið á þeim stöðluðu skilgreiningum, kröfum og ferlum sem traustþjónustuveitendum er skylt að fylgja eins og áður hefur verið tæpt á. Skilgreiningar einar og sér settar fram í reglugerðum og stöðlum duga hins vegar ekki til. Til þess að tryggja að traustþjónustuveitendur fylgi þessum kröfum og ferlum hefur verið er sett á fót skilvirkt eftirlitsferli sem byggir annars vegar á reglubundnu ytra eftirliti samræmismatsaðila, sem hefur það hlutverk að meta hvort starfsemi traustþjónustuaðilans samræmist reglugerðinni og hins vegar á starfsemi eftirlitsaðila á vegum aðildarríkisins þar sem traustþjónustuaðilinn hefur staðfestu. Eftirlitsaðilinn hefur það hlutverk að taka á móti og yfirfara samræmismatsskýrslur, samþykkja umsóknir og fylgjast með starfsemi traustþjónustuaðila að öðru leyti, í samræmi við ákvæði reglugerðarinnar. Það er svo hlutverk landsbundinna eftirlitsaðila að viðhalda traustlistum með upplýsingum um traustþjónustuveitendur og miðla þeim upplýsingum til Evrópusambandsins.

NIÐURLAG

Frumvarp til innleiðingar á þessari reglugerð inn í íslenskan rétt er í smíðum í atvinnuvega- og nýsköpunarráðuneytinu og standa vonir til þess að það verði reiðubúið til framlagningar fljótlega eftir að ný ríkisstjórn tekur við að loknum kosningum. Það verður svo í höndum þess stjórnmálamanns sem þar tekur sæti að taka ákvörðun um framlagninguna sem slíka.

Reglugerðin, verði hún innleidd í íslenskan rétt, mun hafa töluverð áhrif á Íslandi, eins og í öðrum EES ríkjum, ekki síst á þann veg að mun fleiri aðilar munu teljast traustþjónustuveitendur en samkvæmt eldri skilgreiningum. Reglugerðin skapar jafnframt tækifæri fyrir upplýsingatæknifyrirtæki til þess svara þörfum viðskiptavina með nýjum hætti.

Framhaldið er þess vegna í okkar höndum, okkar sem starfa í upplýsingatæknigeiranum að svara kalli ESB og þróa vörur sem hjálpa lögfræðingum að auka traust sitt á rafræna ferla. Hvaða vörur það gætu verið er efni í annan pistil sem verður að bíða síðari tíma.

ÆFINGAR Á REKSTRAR-SAMFELLU FYRIRTÆKJA VIÐ TÖLVUINNBROT

Valdimar Óskarsson, framkvæmdastjóri Syndis

VAXANDI HÆTTA TÖLVUGLÆPA

Hætta vegna tölvuárása og kostnaður sem af þeim hlýst er sífellt að aukast. Engin landamæri eru á Internetinu og þeir sem stunda fjársvik eða þjófnað geta því stundað sína starfssemi óáreitt frá öðrum heimsálfum en sjálft fórnarlambið er búsett í. Með tilkomu rafmiðla eins og Bitcoin er einnig auðveldara fyrir þessa glæpamenn að stunda sína starfsemi þar sem nánast er útilokað að rekja peningaslóðina.

Árásir eru margskonar, allt frá einföldum fjársvikum (e. CFO fraud) yfir í gagnastuld eða jafnvel yfirtaka á heilu tölvukerfunum. Tölvuglæpir taka líka stöðugum breytingum auk þess að tæknilegur metnaður tölvuglæpamanna virðist aukast með hverju ári. Kostnaður við tölvuinnbrot eykst einnig og samkvæmt Forbes [1] er áætlað að heildarkostnaður á heimsvísu árið 2019 verði 2 trilljónir dala. Hvort slíkar spár rætast er ómögulegt að segja til um en ljóst er að þessi tala hefur hækkað gríðarlega á seinustu 5 árum og mun hækka um ókomna framtíð.

VARNARLEYSIÐ ER ALGJÖRT

Syndis er tölvuöryggisfyrirtæki og hefur oft veitt fyrirtækjum neyðarþjónustu þegar tölvuinnbrot hafa átt sér stað. Ef að atvikið er alvarlegt, sérstaklega atvik sem kunna að rata í fjölmiðla, þá er varnaleysi fyrirtækja oftast algert. Þetta eru atburðir sem engum datt í hug að gæti gerst í raun og veru. Stjórnendur og tæknimenn átta sig á því að þó árásinni sé beint gegn fyrirtæki þá er þetta persónulegra en þá hefði órað fyrir og það veldur miklu álagi á þá sem verða fyrir slíku.

Óvissan er oft verri en varnarleysið, þú veist að tölvuinnbrot hefur átt sér stað, en ekki er vitneskja til staður um hvernig það gerist eða hvaða afleiðingar það getur haft. Það er erfitt og tímafrekt að greina afleiðingar tölvuinnbrota en fjölmiðlafulltrúar og stjórnendur vilja gjarnan senda út tilkynningar en í besta falli er hægt að senda frá sér yfirlýsingar eins og: “líkur benda til” þar sem afleiðingarnar eru með öllu óþekktar. Engin tvö tölvuinnbrot eru eins, rannsaka þarf atburði frá byrjun til enda og reyna að endurskapa atburðarásina út frá daufum fingraförum.

AF HVERJU SKIPTA ÆFINGAR MÁLI?

Æfingar eru ein leið til að upplifa að hluta þá tilfinningu sem á sér stað við tölvuinnbrot auk þess að meta viðbrögð og hversu vel fyrirtæki og einstaklingar eru undirbúin til að bregðast við erfiðum aðstæðum af þessum toga. Mörg fyrirtæki setja sér öryggisstefnu og gera æfingar á rekstrarsamfellu gegn jarðskjálftum eða rafmagnsleysi. Æfingar á alvarlegu tölvuinnbroti eru hugsaðar á sama hátt og hjálpa fyrirtækjum að fara í gegnum sína ferla, hagsmunamat, og jafnvel siðferðislegar spurningar sem geta komið upp við slíkar aðstæður.

Flest fólk skilur hefðbundið innbrot í húsnæði auk þess sem flóð eða rafmagnsleysi skilja eftir sig ummerki sem flestir þekkja. Þetta er ekki endilega eðli tölvuinnbrota þar sem afleiðingarnar eru fyrst og fremst að kerfi verða óstarfhæf eða gögnum hefur verið lekið eða breytt, hvernig það gerðist er ekki sýnilegt berum augum. Má sem dæmi segja að ef brotist er inn í skartgripabúð að nóttu til mætti hugsanlega sjá ummerki á hurð eða glugga auk þess að skartgripir hafa verið teknir. Með tölvuinnbrot eru ummerkin ekki eins augljós þó áhrif tölvuinnbrotsins geti verið mjög alvarleg. Þetta er algengt vandamál með flest tölvuinnbrot og því mikilvægt að þjálfa stjórnendur og tæknimenn í réttum viðbrögðum.

SETTU ÞIG Í SPOR GLÆPAMANNSINS

Þegar að æfing á rekstrarsamfellu er framkvæmd, þá er mikilvægt að setja sig inn í þær aðstæður sem eru til staðar en ekki að einblína á tæknileg smáatriði. Til þess að skilja atburðarrásina þá þarf að setja sig í spor tölvuglæpamannsins og endurgera atburðarrásina.

Mikilvæg er að gera sér grein fyrir hvaða gögn eru fyrirtækinu mikilvægust, hver sé tilgangur innbrotsins og hvaða afleiðingar innbrotið geti haft fyrir fyrirtækið. Þar sem svona æfing er ekki byggð á raunverulegu innbroti, þá þarf að setja upp aðstæður sem gætu komið upp ef innbrot hefði átt sér stað. Þessar aðstæður geta verið að tölvuglæpamaður hafi brotist inn og náð í gagnagrunn með upplýsingum um viðskiptamenn og hóti að birta upplýsingarnar opinberlega nema gegn hárri greiðslu í rafmynt. Til að gera æfinguna raunverulegri þá er gott að setja inn skjámyndir úr innri kerfum, þetta auðveldar starfsmönnum að skilja hvað viðkvæm gögn eru í raun og eykur vitund þeirra á hugsanlegum aðstæðum er kunna að myndast við tölvuinnbrot.

Þegar einhver hefur stolið viðkvæmum gögnum þá er ljóst að alvarlegt tjón hefur átt sér stað og mikil óvissa ríkir um afleiðingarnar. Við slíkar aðstæður er mikilvægt að haga aðgerðum á skipulagðan og skilvirkan hátt og má þar nefna hluti eins og:

- Kalla til hagsmunaðila
- Mat á alvarleika tölvuinnbrots
- Aðgerðir og rannsóknarvitund
- Upplýsingaflæði og samskipti
- Mat á vörnum og leiðum til úrbóta

Syndis hefur komið að slíkum æfingum hjá nokkrum viðskiptavinum og er það sameiginlegt mat að svona æfingar geri fyrirtæki betri í að bregðast við, á skilvirkan hátt, ef og þegar að tölvuinnbrot eiga sér stað.

HEIMILD

[1] https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#8b5cd303a913

DNS THREATS TO NETWORK AVAILABILTY

Jo Van Schalkwyk, Content Specialist, Men & Mice

NETWORK AVAILABILITY HAPPENS WHEN IP MEETS DNS

What's your IP address? Chances are you don't know, but without your IP address contacting the IP address of the domain hosting this content, you and I won't be having this conversation. IP addresses, in short, are the phone numbers of the internet.

Since most people aren't that good at remembering large numbers, let alone the 32-bit (IPv4) or 128-bit (IPv6) numbers denoting IP addresses, the internet's forefathers were wise enough to devise a system translating alphabetic names into numerical IP addresses. So to catch up on the latest Trump scandal, we can just enter the easy-to-remember name bbc.com into our web browser, instead of using the hard-to-remember IP address 212.58.244.71. The browser will automatically look into the internet 'directory' to figure out the correct IP address to 'call'.

This almost instantaneous IP address lookup is performed by the Domain Name System (DNS), which, for IP Addresses, works like a large and distributed directory assistant. Whenever any of the billions of daily online requests for information or services are made, appropriate DNS servers spring into motion and answer queries, resolving IP addresses to names and establishing critical connections between those who provide products and services and those who use them.

WHEN DNS FAILS

What happens when DNS becomes unavailable? Well, quite simply, to the user it will appear as if the service they're trying to reach has vanished off the internet. Which, in its turn, can lead to absolutely disastrous repercussions for the providers of products and services. The hard costs [1] of DNS failure, depending on aspects such as your organizational size, type of operations, critical data, backup and recovery systems and number of employees affected, can run up to anything between $55,000 in lost revenue per year for small enterprises, to upwards of $1,000,000 for large companies. The soft costs, such as loss of reputation and customer churn rate, can be just as devastating.

Critical as it is, DNS is also a remarkably vulnerable system, which makes it an attractive target for cyber criminals, often in the form of distributed denial-of-services (DDoS) [2] attacks. A DDoS attack occurs when multiple compromised computer systems flood a server, website or other network resource with messages, connection requests or malformed packets. This slows down, or even crashes the service, rendering it useless for legitimate users or systems.

Late last October, Dyn, provider of DNS to high-traffic domains such as Twitter and Netflix, fell victim to the biggest DDoS attack [3] to date. Making headlines everywhere, Dyn's devastating encounter with, amongst others, the Mirai botnet literally led to every IT team and their data center rethinking how they do DNS, and for good reason - Dyn had enjoyed a whole 8 years of 100% uptime before the 21st of October 2016.

DDoS attacks may be unpredictable, nasty and expensive, but they are not the greatest threat to network availability. Networks are still most vulnerable to simple human and mechanical error, a situation made worse by poor network architecture design and the lack of well-constructed and well-tested disaster recovery plans. Additionally, as technological disruption accelerates, the complexity of systems becomes inflated, requiring both a superior skilled workforce as well as increasingly sophisticated equipment.

British Airways (BA) [4] recently discovered the glaring gaps in their network management the hardest way when a power outage at their main Heathrow data center left 75,000 passengers in 170 countries stranded for days. What most surprised people in the IT industry [5], and not the least BA themselves, was the complete failure of their back-up system to kick in.

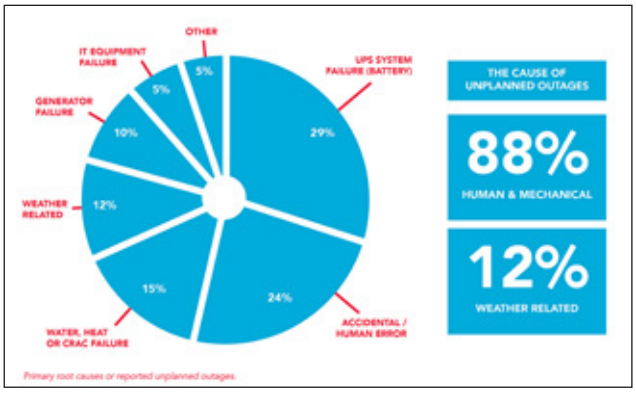


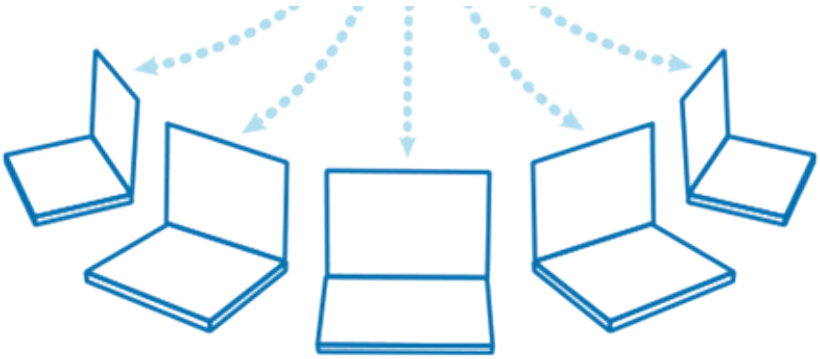
Figure 1 – the main causes of outages in data centers (source: data from Vertiv, formerly Emerson Network Power [6])

BA's woes serve as an unpleasant, but urgent, reminder that the way we back up our systems is sometimes even more critical than how we run it day-to-day. As it goes with life insurance or a last will and testament, there's no point in waiting until your plane goes down (or fails to go up) before you start getting your house in order.

KEEPING YOUR DNS UP AND RUNNING, ALWAYS

In the last decade or so, the creation of anycast [7] technology and large-scale cloud services have allowed companies to dump the cost and complexity of running their own DNS in favor of the generally much better network availability, load distribution and systems back-up of highly specialized DNS [8] service providers.

Yet, as seen in the case of Dyn last October, putting all your DNS availability eggs in one DNS basket, however specialized it is, is not necessarily the most secure solution. Looking at the odds and costs of outages, many enterprises are now opting to bring in a second, or even a third, DNS service to hold copies of critical DNS master zones. That way, if your sole source of external DNS is knocked out due to power



failure, human error or malicious cyber activity, this critical service is still active, ensuring service continuity and retaining critical operational data – and if you're BA, keeping your passengers happy in the air, instead of sleeping on yoga mats in conference centers.

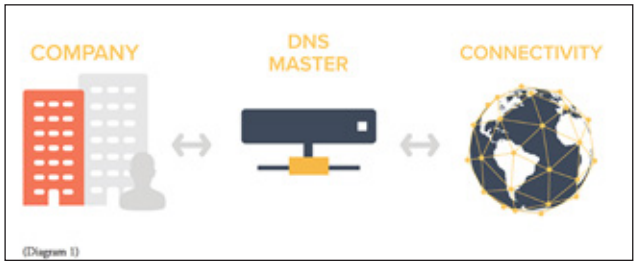


Figure 2 - External DNS redundancy

This system of external DNS redundancy [9] boosts DNS availability by:

1. removing the danger of exposure to a single point of DNS failure.
2. reducing traditional master-slave DNS redundancy vulnerabilities, where slave zones can't be changed if the master becomes unavailable.
3. improving infrastructure resilience by hosting critical zones with multiple providers, ensuring continued service availability and updates of changes if one DNS service provider becomes unavailable.

Additionally, maintaining redundant DNS at more than one provider helps you to avoid the pitfalls of vendor lock-in.

HOW TO MULTI-DNS: THINK COMPATIBILITY ACROSS PLATFORMS, THINK AUTOMATION

In theory, DNS redundancy across multiple DNS service provider platforms should be the best solution for optimal DNS high reliability, high availability and high performance. In practice, however, the complexity of tasks and scope for error involved in replicating and maintaining identical DNS zones on multiple platforms pose additional threats to DNS availability. The situation is made worse by:

- A lack of centralized views
- A lack of workflow automation
- The difficulty of coordinating multiple platform APIs

Maintaining and keeping DNS records in sync in multiple host locations is complicated, but can be done using APIs or custom applications. However, it's important to choose DNS service providers that offer similar functionalities and are able to operate in a collaborative setting. Also consider the global points of presence (PoP) of the providers, the quality of their APIs and reporting tools and their performance in different locations and under varying server load. You want to be able to deploy your multi-DNS on different networks - your service providers should be capable of seamless integration through APIs or custom programs.

To reduce complexity and ease the replication and synchronization of data across multiple DNS platforms, it also pays to explore third-party solutions such as Men & Mice's xDNS redundancy [10].

THE BIGGER PICTURE

Apart from covering all your bases by deploying well-architectured multi-DNS, it's worth taking a look at other ways of mitigating DDoS and preventing DNS failures at large. Geoff Huston made an impassioned plea for stepping up DNSSEC deployment at RIPE 73 [11] and DPRIVE, the DNS PRIVate Exchange Working Group, is working on developing mechanisms [12] to enable the confidentiality of DNS transactions. Other groups, such as the Internet Society, is charting a number of initiatives [13], aimed at, for instance, creating a more secure environment surrounding the Internet of Things.

It is said that the price of freedom is eternal vigilance. Making the internet more secure, but keeping it an open and free network of networks, without any single entity exercising centralized control, will require collective solutions and a collaborative security [14] effort. I guess we better get going at it.

HEIMILDIR

[1] http://www.spotmigration.com/blog/how-much-does-network-downtime-really-cost/
[2] http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
[3] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[4] https://www.theguardian.com/business/2017/may/29/ba-computer-crash-passengers-face-third-day-of-disruption-at-heathrow
[5] http://www.bbc.com/news/business-40082631
[6] https://journal.uptimeinstitute.com/data-center-outages-incidents-industry-transparency/
[7] http://ddiguru.com/blog/118-introduction-to-anycast-dns
[8] https://www.internetsociety.org/blog/tech-matters/2016/10/how-survive-dns-ddos-attack-consider-using-multiple-dns-providers
[9] http://info.menandmice.com/blog/keep-it-outages-off-your-network-with-redundant-dns
[10] http://info.menandmice.com/blog/secure-your-dns-across-multiple-dns-service-platforms-with-men-mice-xdns-redundancy
[11] https://ripe73.ripe.net/archives/video/1536/
[12] http://info.menandmice.com/blog/ready-for-another-look-at-dnssec
[13] https://www.internetsociety.org/blog/tech-matters/2016/10/trust-isnt-easy-drawing-agenda-fridays-ddos-attack-and-internet-things
[14] https://www.internetsociety.org/collaborativesecurity

THE NEW ADVANCED PULSATING THREATS

Charlie Eriksen, a principal security engineer at Syndis

For years, the media has been obsessed with nation state-sponsored hacking, also known as „Advanced Persistent Threats“ (APT). APT is a term, which within IT circles, is now common-place, yet most people have no reason to really care about it. But as the Internet of Things (IOT) gets more widespread, there's a new type of APT that can shake the very foundation of some people's private life: The Advanced Pulsating Threat, also known as „Smart Toys“, or „Smart Vibrators“, i.e. adult toys with smart functionality.

If these are foreign concepts to you, fear not. After discussing at UTMessan 2017 the dangers of these smart toys, I was universally met with surprise from people, who not only had never heard of these types of products, or realized that what had been demonstrated in the presentation was something, which they had, be worried about. Whether it seems likely that seemingly nobody had heard of these products before the presentation, I leave up to the reader to determine. However, regardless, not having realized the potential risks to privacy and health that these products pose is probably the only reasonable reaction in this case, unless one is exceedingly paranoid.

If one browses a store that sells adult toys, one will quickly find numerous “smart” products. These feature everything from wireless radio-frequency remotes (often operating at the same 2.4GHz frequency as WiFi, and microwave ovens), to toys with fully-fledged apps. These allow not only the user themselves to control the toy, but also for granting control to other users with the app, such as a partner who's abroad.

As an inherently curious mind, and as somebody who gets paid to hack things for a living, it was impossible to simply walk by one of these things on a shelf, and not get an itch to try to hack it. After discussing this at lunch one day at the office, resulting in constant, unrelenting adult-themed jokes, it was decided that this would be exciting to hack. A bit of research quickly uncovered, that very little had been published on this subject, so a company expense w a s filed to buy one of these devices, and get right on hacking it!

The device we had purchased featured a smartphone app, which controls it using bluetooth. To set it up, you connect to the device as if it was a bluetooth speaker, and then open the app. Then you can pick speeds and patterns amongst other things. Alternatively, since it presents itself as a speaker, you can also play music with it, or take a call. We do however not recommend either, given that the speaker has been replaced with a vibrating motor, which makes it impossible to conduct an intelligent conversation, be it with your boss, or family member. In addition, everybody may, not appreciate trying to communicate through a vibrator.

If one wishes to use some of the more advanced features, you have to sign up for an account with the app. One has to pick a nickname, such that others can find you from the app, and of course, the mandatory providing your email address, and pick a password. You are even able to upload a profile image, should one wish to display one's personality, when others see your name in the profile search list.

Having signed in, we were also given the option of pressing a button, to indicate to the app, that we had an orgasm. The app would then track these for us, and set goals for the year, as to having regular orgasms. However, initially we did not care about that beyond having a giggle, since we were mostly interested in hacking the actual control of the vibrator. So we quickly moved onto investigating how the user-to-user control worked. We loaded up all the tools we use for testing mobile applications, connected two phones over the app together, and got started.

Nevertheless, things did not go according to plan. Something very strange was happening, suggesting that our test setup was broken. Our tools were able to see, in plain text, all the communication between the two devices. We had not yet actually configured our tools in a way, to “hijack” the encrypted HTTPS channels we expected the application to make. Expecting the problem to exist between the computer, vibrator, and chair, we spent hours trying to determine what had gone wrong. Eventually, we figured out that we had done nothing wrong at all.

Rather, we had discovered that the app-to-app communication was being done very unencrypted. This communication channel was used to control pattern/strength of the vibration, as well as allowing for sending of messages, images, and such. Anybody sniffing the local wireless would see that, and be able to assume control over the device. Yikes! Not only that, when trying to establish the app-to-app connection, it would send you the email address of the user you tried to connect. Combine this with the ability to easily scrape a list of all usernames that have signed up to the app, it would be trivial to then also create a script to get all the associated email addresses.

And that's where this research, initially mostly done for laughs, really rocked our world. This seemingly “innocent” toy turned out to be not only tracking information about your usage of the product, and send it to the cloud out of your control. It also opened users up to a violation of their expected privacy. Here in Iceland, the subject of sexuality is far less taboo than many parts of the world. But even then, it's clear from talking to a lot of people about this research, that if somebody had abused the weaknesses we discovered, and published the data, that it could have created some seriously awkward situations for people, if not outright dangerous.

Therefore, it is critical that, as these types of “smart” things invade every aspect of our lives, consumers are aware of the privacy implications that they pose, if companies are not held responsible for the data they collect, and store. In addition, that the products they sell, are not inherently insecure out of the box.

If this is not addressed, we may end up living in a world where not only would you have to worry about your usage data of adult toys being leaked to the public. But also that somebody malicious may hijack the control of the device you use for pleasure, and just turn it to 11 unexpectedly, which only the truest of masochists would enjoy. And when it comes to privacy, and security, collective masochism is not the way forward.

ÞAÐ ER ENGU LÍKT AÐ SIGRAST Á ERFIÐUM ÁSKORUNUM

Við stöndum ávallt frammi fyrir krefjandi og skemmtilegum verkefnum

ÁRNASYNIR

Við viljum eingöngu hafa í okkar röðum forritara, tækni- og rekstrarfólk í fremstu röð enda starfar margt af öflugasta tæknifólki landsins hjá okkur.

Við erum að tala um einstaklinga sem við treystum fyrir lyklinum að mikilvægustu upplýsingakerfum landsins. Það eru ekki margir sem uppfylla þau skilyrði, ert þú ein/n af þeim?

Við erum alltaf til í að heyra í hæfileikaríku fólki. Endilega sendu inn umsókn á www.rb.is.

REIKNISTOFA BANKANNA | Höfðatorg | Katrínartúni 2 | 105 Reykjavík | Sími: 569 8877 | www.rb.is

HLUTVERK OG SKYLDUR VINNSLUAÐILA Á GRUNDVELLI NÝRRA PERSÓNUVERNDARREGLNA

Lena Markusdóttir, Ingvi Snær Einarsson og Erla S. Árnadóttir, sérfræðingar LEX á sviði persónuverndar og upplýsingatækniréttar

Margir lesendur Tölvumála vita vafalaust af setningu nýrra persónuverndarreglna í Evrópu. Nánar tiltekið er um að ræða reglugerð ESB nr. 2016/679 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin). Reglugerðin öðlaðist gildi 24. maí 2016 og kemur til framkvæmda innan ESB frá og með 25. maí 2018. Á Íslandi verður reglugerðin innleidd á grundvelli EES-samningsins og í kjölfarið mun ný persónuverndarlöggjöf taka gildi, en áætlað er að það verði á árinu 2018 [1].

Reglugerðin hefur í för með sér ýmsar breytingar sem meðal annars snerta hina svonefndu vinnsluaðila og verður hér gerð grein fyrir helstu breytingunum. Samantektin er byggð á greiningu á reglugerðinni sjálfri, núgildandi lögum og þegar það á við á álitum hins svokallaða 29. gr. starfshóps sem hefur að undanförnu látið í té nokkur álit á einstökum efnisatriðum sem reglugerðin tekur til [2].

HVERJIR ERU VINNSLUAÐILAR?

Vinnsluaðili er skilgreindur sem einstaklingur eða lögaðili, opinbert yfirvald, sérstofnun eða annar aðili sem vinnur persónuupplýsingar á vegum ábyrgðaraðila, en ábyrgðaraðili er sá sem sem ákvarðar tilgang og aðferðir við vinnslu persónuupplýsinga. Til að mynda teljast upplýsingatæknifyrirtæki hvers konar sem varðveita persónuupplýsingar á vegum annarra eða hafa aðgang að þeim með öðrum hætti til vinnsluaðila [3]. Líkt og núgildandi lög gera ráð fyrir skal gerður vinnslusamningur milli ábyrgðar- og vinnsluaðila, en almenna persónuverndarreglugerðin gerir nákvæmari og ítarlegri lágmarkskröfur til efnis slíkra vinnslusamninga sem fara ætti vel yfir við gerð þeirra. Rétt er að benda á að ekki er mælt fyrir um að ákvæði eldri reglna skuli áfram gilda um vinnslusamninga sem nú þegar eru í gildi og þurfa þeir því einnig að standast kröfur nýju reglugerðarinnar. Yfirfara ætti því alla slíka samninga og eftir atvikum ganga frá uppfærðum vinnslusamningum.

VIÐBÓTARVINNSLUAÐILAR

Vinnsluaðilar geta ráðið aðra aðila til að inna tiltekna vinnslustarfsemi af hendi fyrir hönd ábyrgðaraðila, svonefnda viðbótarvinnsluaðila. Viðbótarvinnsluaðilar þessir geta verið af ýmsu tagi, t.d. aðili sem starfrækir gagnaver sem vinnsluaðili nýtir til hýsingar persónuupplýsinga sem hann vinnur á vegum ábyrgðaraðila. Vinnsluaðilum er aðeins heimilt að nýta viðbótarvinnsluaðila að fengnu skriflegu samþykki frá ábyrgðaraðila. Þá er mælt fyrir um skyldu vinnsluaðila til að gera samninga við viðbótarvinnsluaðila og ganga úr skugga um að tæknilegar og skipulagslegar ráðstafanir standist kröfur reglugerðarinnar, en vinnsluaðilar bera fulla ábyrgð gagnvart ábyrgðaraðilum á því að viðbótarvinnsluaðilar efni skuldbindingar sínar.

INNBYGGÐ OG SJÁLFGEFIN PERSÓNUVERND

Með innbyggðri persónuvernd er átt við að vernd persónuupplýsinga sé innbyggð í vörur og þjónustu, t.a.m. að hugbúnaður sem notaður er við vinnslu sé hannaður á þann hátt að aðeins þeim upplýsingum sem nauðsynlegar eru til að uppfylla tilgang vinnslunnar sé safnað. Með sjálfgefinni persónuvernd er átt við að það sé sjálfgefið að persónuupplýsingar verði ekki gerðar aðgengilegar almenningi án íhlutunar einstaklingsins sem persónuupplýsingarnar varða. Ef notaðir eru vinnsluaðilar við vinnslu persónuupplýsinga þarf ábyrgðaraðili að ganga úr skugga um að vinnslan uppfylli þessar kröfur. Vinnsluaðilar sem eru upplýsingatæknifyrirtæki og koma að hönnun og þróun hugbúnaðar þurfa að hafa þessar reglur sérstaklega í huga [4].

SKRÁ YFIR VINNSLUSTARFSEMI

Vinnsluaðilar skulu halda skrá yfir alla flokka vinnslustarfsemi sem framkvæmd er fyrir hönd ábyrgðaraðila og gera hana aðgengilega eftirlitsyfirvaldi að beiðni þess, en skylda þessi er nýnæmi með tilkomu reglugerðarinnar. Í reglugerðinni eru talin upp þau atriði sem skráin þarf að innihalda. Þetta eru atriði á borð við samskiptaupplýsingar um vinnsluaðilann, sérhvern ábyrgðaraðila sem hann starfar fyrir og almenna lýsingu á öryggisráðstöfunum sem viðhafðar eru við vinnsluna [5]. Frá þessari skyldu gildir sú undantekning að fyrirtæki eða stofnanir sem hafa færri en 250 starfsmenn þurfa ekki að halda skrá yfir vinnslustarfsemi nema vinnsla sé líkleg til að hafa í för með sér áhættu fyrir réttindi og frelsi skráðra einstaklinga, vinnslan sé ekki tilfallandi eða taki til viðkvæmra persónuupplýsinga. Það má gera sér í hugarlund að undantekningin muni eiga óvíða við þar sem skilyrðum þess að henni megi beita eru settar afar þröngar skorður.

ÖRYGGI PERSÓNUUPPLÝSINGA

Vinnsluaðilar skulu gera viðeigandi tæknilegar og skipulagslegar ráðstafanir sem tryggja viðunandi öryggi persónuupplýsinga sem þeir hafa með höndum. Með tilkomu reglugerðarinnar tekur skylda þessi nú beinlínis til vinnsluaðila en ekki einungis í gegnum ábyrgðaraðila líkt og áður. Í reglugerðinni eru sérstaklega nefndar nokkrar ráðstafanir sem notast ætti við eftir því sem við á, t.a.m. notkun gerviauðkenna (e. pseudonymisation) og dulkóðun persónuupplýsinga. Vinnsluaðilar ættu því að ganga úr skugga um hvort núverandi tæknilegar og skipulagslegar ráðstafanir veiti persónuupplýsingum viðeigandi vernd eða hvort gera þurfi breytingar áður en ný löggjöf tekur gildi.

TILKYNNING UM ÖRYGGISBROT

Með öryggisbroti er átt við brot á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar, glötunar, breytinga eða birtingar persónuupplýsinga eða aðgangur að þeim veittur í leyfisleysi. Ef vinnsluaðili verður var við öryggisbrot við



meðferð persónuupplýsinga ber honum að tilkynna það til ábyrgðaraðila án ótilhlýðilegrar tafar. Það er svo á hendi ábyrgðaraðila að tilkynna öryggisbrotið til eftirlitsyfirvaldsins innan 72 klukkustunda frá því hann varð atburðar var. Tímafrestirnir eru því naumir og ekki fullljóst hvernig túlka ber samspil tímafresta sem vinnslu- og ábyrgðaraðilum eru gefnir í reglugerðinni. Líklega byrjar 72 klukkustunda festur ábyrgðaraðila að líða frá tíma tilkynningar vinnsluaðila, sem berast skal án ótilhlýðilegrar tafar, ef það er jafnframt sá tímapunktur sem ábyrgðaraðili fyrst veit af öryggisbroti sem á sér stað hjá vinnsluaðila. Vænta má nánari leiðbeininga um tilkynningar vegna öryggisbrota frá 29. gr. starfshópnum á þessu ári [6].

PERSÓNUVERNDARFULLTRÚAR

Tilnefning persónuverndarfulltrúa hefur ekki tíðkast áður hér á landi, en þekkist í sumum nágrannalöndum okkar, t.d. í Noregi og Þýskalandi. Með tilkomu nýju persónuverndarreglnanna skulu allir opinberir aðilar og þeir einkaaðilar sem hafa sem meginstarfsemi vinnsluaðgerðir sem krefjast umgangsmikils, reglubundins og kerfisbundins eftirlits með einstaklingum eða umfangsmikla vinnslu viðkvæmra persónuupplýsinga, tilnefna persónuverndarfulltrúa. Vinnsluaðilar verða nú að meta hvort þeir uppfylli ofangreind skilyrði og að á þeim hvíli þar með skylda til að tilnefna persónuverndarfulltrúa. Þá skal bent á að aðildarríkjum er einnig heimilt að ákveða með lögum að tilnefna skuli persónuverndarfulltrúa í öðrum tilvikum en þeim sem að framan greinir, og því er mælt með að fylgst sé náið með lagasetningu hvað þetta varðar. Persónuverndarfulltrúinn getur verið starfsmaður eða utanaðkomandi aðili og skal hafa sérþekkingu á persónuverndarlöggjöf að teknu tilliti til vinnslunnar sem fram fer hjá aðilanum. Persónuverndarfulltrúinn þarf því bæði að hafa þekkingu á gildandi lögum og framkvæmd sem og vinnslustarfsemi aðilans, en ekki er gerð krafa um tiltekna menntun. Helstu verkefni persónuverndarfulltrúans eru upplýsingagjöf og eftirlit með að farið sé eftir gildandi persónuverndarlögum, og er hann einnig tengiliður fyrir eftirlitsyfirvöld og einstaklinga. Persónuverndarfulltrúinn skal vera sjálfstæður í störfum sínum og heyrir beint undir æðstu stjórn aðilans. Hann getur gegnt öðrum störfum svo lengi sem þau leiða ekki til hagsmunaárekstra og má þ.a.l. alla jafna ekki vera framkvæmdastjóri, mannauðsstjóri, markaðsstjóri eða gegna annars konar stöðu þar sem hann ákvarðar tilgang og aðferðir við vinnslu persónuupplýsinga. Þá má ekki refsa honum eða víkja úr starfi fyrir framkvæmd verkefna sinna sem persónuverndarfulltrúi. Viðkomandi ábyrgðar- eða vinnsluaðili ber áfram ábyrgð á að lögunum sé fylgt.

MIÐLUN PERSÓNUUPPLÝSINGA TIL ÞRIÐJU LANDA

Reglur um miðlun persónuupplýsinga til þriðju landa, þ.e. landa sem ekki veita persónuupplýsingum sambærilega vernd og samkvæmt persónuverndarreglugerðinni, eiga beinlínis við um vinnsluaðila með tilkomu nýju reglnanna. Vinnsluaðilar þurfa því að athuga hvort slík miðlun eigi sér stað, t.a.m. með notkun gagnavera og skýjaþjónusta eða til fyrirtækja innan samsteypu, og hvort hún samrýmist heimildum nýju reglnanna.

STJÓRNSÝSLUSEKTIR O.FL.

Vinnsluaðilar geta samkvæmt almennu persónuverndarreglugerðinni borið sjálfstæða ábyrgð og orðið ábyrgir til jafns við ábyrgðaraðila ef reglunum er ekki fylgt, en hingað til hefur ábyrgðin gagnvart eftirlitsyfirvöldum og einstaklingum legið eingöngu hjá ábyrgðaraðilum. Ber þar helst að nefna heimildir eftirlitsyfirvalda til að leggja á stjórnsýslusektir vegna brota á reglunum sem geta numið þeirri fjárhæð sem hærri er, 20 milljónum Evra eða 4% af árlegri heildarveltu á heimsvísu á næstliðnu fjárhagsári. Einnig getur vinnsluaðili borið bótaábyrgð vegna tjóns sem hlýst af vinnslu sem brýtur í bága við reglugerðina eða ef hann hefur farið gegn lögmætum fyrirmælum ábyrgðaraðila.

HEIMILDIR

[1] Sjá heimasíðu Persónuverndar, t.d. https://www.personuvernd.is/ny-personuverndarloggjof-2018/fyrir-logadila/ (sótt 3.5.2017).

[2] e. Article 29 Working Party. Starfshópnum var komið á fót með núgildandi tilskipun og er skipaður fulltrúum frá persónuverndarstofnunum aðildarríkjanna á EES-svæðinu auk fulltrúum framkvæmdastjórnar ESB og hins evrópska persónuverndarfulltrúa. Hópurinn gegnir ráðgefandi hlutverki og hefur gefið út leiðbeiningar um ýmis lykilákvæði núgildandi tilskipunar og nú einnig almennu persónuverndarreglugerðarinnar.

[3] Hér er rétt að benda á að vinnsluaðilar geta á sama tíma verið ábyrgðaraðilar gagnvart tilteknum persónuupplýsingum, t.d. um eigið starfsfólk.

[4] Um nánari umfjöllun vísast til greinarinnar „Innbyggð og sjálfgefin friðhelgi í upplýsingakerfum – er þitt fyrirtæki tilbúið?“ eftir Ölmu Tryggvadóttur og Vigdísi Evu Líndal sem birtist í 1. tbl. 40. árg. Tölvumála í nóvember 2015.

[5] Hér gefst ekki ráðrúm til að fara yfir öll atriðin, en vísað er til 2. mgr. 30. gr. almennu persónureglugerðarinnar þar sem upptalninguna er að finna.

[6] Sjá t.d. https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/01/ Pressrelease-Adoptionof2017GDPRActionPlan.pdf (sótt 3.5.2017).

AÐ SETJA SIG Í SPOR MÓTHERJANS

James Elías Sigurðarson, security developer, Syndis

Á hverjum degi tengjast fleiri og fleiri „tæki“ Internetinu, allt frá brauðristum til sjálfkeyrandi bíla. Talið er að um 200 billjón tæki munu vera nettengd árið 2020[1]. Líf okkar í dag á sér stað að miklu leyti á netinu, meðal annars á samfélagsmiðlum, í afþreyingu, verslun o.fl. Samhliða þessari þróun þá hafa tölvuárásir orðið sívaxandi vandamál. Á minna en ári hefur heimsbyggðin upplifað stærstu DDoS árás allra tíma [2], tölvuþrjótar hafa tekið yfir heilbrigðiskerfi [3], og nýjar árásir eiga sér stað á hverjum degi. Tölvuöryggi er því nú þegar mikilvægur hluti af okkar daglegu lífi og verður enn mikilvægari í komandi framtíð.

HVAÐ ER HÆGT AÐ GERA TIL AÐ BÆTA TÖLVUÖRYGGI?

Þetta er stór spurning sem er erfitt að svara á fullnægjandi hátt í stuttu máli, en við skulum einbeita okkur að rót vandans, sem má segja að liggi milli stóls og lyklaborðs. Fyrir utan mannlegan breyskleika og hversu ginnkeypt fólk virðist vera fyrir gylliboðum Internetsins þá eru tölvuárásir að miklu leyti drifnar áfram á veikleikum í hugbúnaði. Slíka öryggisveikleika má í mörgum tilfellum rekja til mannlegra mistaka í þróunarferli hugbúnaðar. Því er rétt að athuga hvað hægt sé að gera til að minnka tíðni þeirra.

Ímyndum okkur bílstjóra með almenn ökuréttindi sem er látinn keyra stóran trukk. Hann kann að keyra, en ekki þungan trukk, þar sem maður þarf meðal annars að hugsa um aðrar hættur eins og t.d. lengri stöðvunarvegalengd. Væri allt í lagi að leyfa honum að setjast undir stýri öryggislega séð?

Þetta er því miður staðan í dag er varðar nýútskrifaða tölvunarfræðinga hér á landi og víða erlendis. Nýútskrifaðir tölvunarfræðingar munu forrita mikilvægan hugbúnað í náinni framtíð án þess að hafa öðlast þjálfun í að verja þann hugbúnað gegn öryggisgöllum. Aðeins örfáir áfangar tengdir tölvuöryggi eru í boði á háskólastigi og er enginn þeirra skylda. Þetta er óæskileg staða eins og er, fyrst hugbúnaður geymir persónuupplýsingar í ört vaxandi magni. Glæpamenn og óvinveittar ríkisstjórnir einbeita sér einnig í auknum mæli að tölvuinnbrotum og tölvuglæpum. Því er mikilvægt að allur hugbúnaður sé varinn árásum.

HVERNIG ER HÆGT AÐ ÞJÁLFA FORRITARA Í ÖRUGGARI HUGBÚNAÐARÞRÓUN?

Hver og einn veit best hvernig hvernig hægt er að brjótast inn í eigið hús. Til dæmis veit maður um glugga sem eru ekki með öryggisskynjara og hvar varalykillinn er geymdur. Þetta má heimfæra á forritara. Forritari sem skrifar hugbúnað er í bestu stöðunni til að finna öryggisveikleika í eigin hugbúnaði. Þetta mótar mikilvæga aðferð til að sporna gegn öryggisgöllum, að þjálfa forritara og efla vitneskju á öryggisgöllum ásamt því að kenna þeim að rýna hugbúnað í leit að öryggisgöllum. Þar með lærir forritarinn að setja sig í spor mótherjans og hvernig best sé að brjótast inn í sinn eigin hugbúnað.

Einn möguleiki til að öðlast slíka þekkingu í dag er í gegnum svokallaðar CTF (e. Capture The Flag) keppnir. Áhugasömum þátttakendum er boðið upp á allskyns þrautir sem innihalda einhvern öryggisgalla sem markmiðið er að leita uppi. Keppandinn þarf síðan að finna hvernig hægt er að nýta öryggisgallann til að stela svokölluðum “fána” sem veitir honum stig. Dæmin sem koma fyrir í þessum keppnum kynna keppandanum fyrir allskyns öryggisveikleikum, bæði nýjum sem og þekktum. Að geta leitað uppi öryggisveikleika er mikilvæg kunnátta sem keppandinn getur nýtt á sinn eigin kóða eða kóða annarra.

Undanfarin tvö ár hefur keppnin IceCTF [4] verið haldin af nemendum Háskólans í Reykjavík með styrkjum frá Syndis og Háskólanum í Reykjavík, og hefur vakið mikla lukku bæði innanlands og erlendis. Markmið keppninnar er að huga að byrjendum í hugbúnaðargerð og kynna þeim fyrir einföldum öryggisgöllum, sem og að kynna nýja öryggisgalla og bjóða þeim sem hafa áhuga á að prófa sig áfram í að reyna á þessa veikleika. Fjöldi þátttakenda hefur farið vaxandi en á síðasta ári tóku 3000 manns þátt og þar af voru 300 íslenskir keppendur.

Þetta er ágæt lausn til að efla öryggisvitund, en virkar einungis á þá sem hafa þekkingu og áhuga á tölvuöryggi og/eða skilja mikilvægi þess í dag. Sá hópur er því miður í minnihluta eins og er og því þarf aðra lausn til að ná til flestra.

HVAÐ MEÐ ALMENNA FORRITARA?

Hægt væri að taka þessa CTF hugmynd og gera hana skemmtilegri, og þar með beina henni að almennum forriturum. Þeir geta þá með einföldu móti fengið að sjá og lifa sig inn í spor tölvuþrjóts sem er að nýta sér þekkta öryggisveikleika. Samtímis er hægt að sýna þeim hvernig sá veikleiki lítur út í kóða og hvernig skal verjast honum.

Þannig myndi tölvuöryggiskennsla verða skemmtilegt námskeið sem gæti meðal annars orðið hluti af skyldunámi í tölvunarfræði í háskólum landsins, annaðhvort sem hluti af öðrum námskeiðum eða sem sér námskeið innan skólans. Tölvuöryggiskennslan myndi kynna verðandi forriturum fyrir þekktum veikleikum og varnir gegn þeim, og þar með loka á þekktar aðferðir sem tölvuþrjótar nota til að brjótast inn í kerfi. Svona nám mun því gera skólunum kleift að skila betri forriturum út á vinnumarkaðinn að námi loknu.

Eins og staðan er í dag þá er þetta ágæt lausn en gallinn er að þær koma eftir á, sem einskonar sérkennsla, sem þarf samt að vera til staðar, en til að ráðast að rót vandans væri best að kenna örugga hugbúnaðarþróun sem hluta af námi forritara. Þar með yrði hugsunarháttur mótherjans innbyggður í forritara framtíðarinnar.

HVERNIG ER HÆGT AÐ MÓTA HUGSUN TÖLVUNARFRÆÐINGA FRAMTÍÐARINNAR?

Einfölduð mynd af öryggisgöllum er að í grunninn séu flestir þeirra forsenda, sem forritarinn heldur að sé sönn, en í ljós kemur að svo var ekki. Til dæmis má nefna að í „Heartbleed“ [5] öryggisgallanum, sem var mjög útbreiddur fyrir nokkrum árum, þá var forsendan sú að enginn myndi senda rangar upplýsingar í „Heartbeat“ skilaboðum til vefþjónsins. Eins og flestir vita, þá reyndist sú forsenda ekki sönn, og því urðu margar

vefsíður opnar fyrir þeim veikleika með alvarlegum afleiðingum. Þetta mótar aðra aðferð til að sporna við öryggisgöllum, að þjálfa forritara í að hugsa vel um hverjar þeirra forsendur eru, og hvort þær séu sannar.

Þessi hugsun getur náð til kennslu í skóla, til dæmis að láta nemendur hugsa vel um hvað gerist ef einhver aðili gerir eitthvað allt annað en kerfin búast við. Þessi hugsunarháttur getur verið hluti af öllum forritunarnámskeiðum í háskólum, og þá verið einna mikilvægasti kostur sem framtíðar tölvunarfræðingur tekur með sér út á vinnumarkað. Ef allir hugsuðu þannig myndi það orsaka að í framtíðar hugbúnaði væri mjög mörgum veikleikum einfaldlega útrýmt, sem gerir það enn erfiðara fyrir tölvuþrjóta að brjótast inn.

Í dag er mikil þróun og mikill flýtir við að koma nýjungum út. Þessar nýjungar móta komandi framtíð þar sem vaxandi hluti gagna okkar mun verða á netinu. Þar af leiðandi er mikilvægt að við, sem þróum þessar nýjungar, setjum okkur í spor mótherjans og lærum að gagnrýna okkar eigin hugbúnað áður en alvöru tölvuþrjótur verður fyrri til.

HEIMILDIR

[1] https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html
[2] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[3] http://telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomwareoffensive/
[4] https://icec.tf/
[5] http://heartbleed.com/

TÖLVUNARFRÆÐI – SÍBREYTILEGT NÁM FYRIR SÍBREYTILEGA FRAMTÍÐ

Viðtal við Dr. Gísla Hjálmtýsson, Háskólanum í Reykjavík
Viðtalið tók Ásrún Matthíasdóttir

Dr. Gísli Hjálmtýsson er nýr deildarforseti tölvunarfræðideildar Háskólans í Reykjavík (HR) en hann starfaði á árum áður við skólann þegar hann var prófessor og forseti deildarinnar 2001-2007. Hann hefur langa reynslu sem frumkvöðull og stjórnandi á sviði upplýsingatækni og nýsköpunar á fjölbreyttum sviðum íslensks og alþjóðlegs viðskiptalífs. Það er alltaf spennandi þegar nýr stjórnandi tekur við og því langaði Tölvumálum að heyra aðeins í Gísla um stöðu tölvunarfræðinnar í dag og framtíðarsýn hans.

FYRST SPURÐI ÉG HANN HVER STAÐAN VÆRI Í DEILDINNI Í DAG?

Háskólann í Reykjavík er orðinn menntastofnun sem Íslendingar eiga að vera stoltir af. Fyrir 15 árum var HR startup – í dag er skólinn á lista yfir bestu háskóla í heimi. Tölvunarfræðideildin hefur að sama skapi þroskast frá því að ég kom 2001 sem fyrsti og eini prófessor skólans, yfir í að vera vel mönnuð bæði til kennslu og rannsókna, og með afrekaskrá sem sæmir mun stærri skólum. Til að mynda eigum við fjóra heimsmeistaratitla í alhliða leikjaspilun (General Game Playing) á síðustu árum, þar sem við keppum við MIT, Stanford og alla stærstu skóla heims, þar sem við mætum til leiks með langminnsta teymið og enn minna af fjármunum. Annað dæmi eru rannsóknir á fælni og umhverfissálfræði með nýtingu sýndarveruleika. Þessi verkefni er brautryðjandi á heimsvísu.

Tölvunarfræði er mjög vinsæl námsgrein, svo mjög að á hverju ári þurfum við því miður að vísa stórum hópi umsækjenda frá. Á sama tíma þurfum við aukinn fjölbreytileika nemenda í tölvunarfræði með fjölbreytt áhugasvið, þekkingu og reynslu. Langvarandi eftirspurn eftir tölvunarfræðingum í heiminum er fyrirsjáanleg og tækifæri til vinnu eða stofnun nýrra fyrirtækja margs konar. Við leitum nú fleiri kennara og rannsakenda til að geta tekið við breiðari hópi af nemendum.

ERU BREYTINGAR Í VÆNDUM Í TÖLVUNARFRÆÐIDEILDAR HR?

Breytingar í tölvunarfræði eru meiri en í flestum greinum, þannig að það er óhjákvæmilegt að bæði nám og rannsóknir séu í stöðugri framþróun. Við erum með nýjungar í kennslu og námsbrautum í deiglunni, m.a. með það fyrir augum að flétta námið í tölvunarfræði saman við önnur svið, t.d. sálfræði, heilbrigðisverkfræði og lögfræði, auk þess sem við bjóðum þegar námsbrautir með viðskiptafræði- og verkfræðideildunum. Ég sé það bara aukast. Þá hyggjumst við nýta enn frekar tölvutækni við kennslu og sjálfnám, og nýta tíma kennarana til að vinna í lausnum og verkefnum með nemendum frekar en í fyrirlestra. Sem fyrr leggjum við áherslu á að nemendur okkar séu gerendur og samtvinnum fræðin og smíði lausna.

AÐ LOKUM, HVER ER ÞÍN FRAMTÍÐARSÝN?

Markmið okkar er að á Íslandi verði blómlegur hátækniiðnaður, sem bæði mótar og styður við atvinnu- og samfélagsþróun á Íslandi. Háskólinn í Reykjavík er nýsköpunarháskóli og í því felst að búa til atvinnulíf framtíðarinnar. Allir þekkja tölur um að meirihluti núverandi starfa muni hverfa á næstu áratugum. Ísland er þar ekki undanskilið. Þrátt fyrir náttúrauðlindir, mun framtíðarhagsæld á Íslandi byggjast á þekkingu og mannauði, en til þess þurfum við að búa til nýjar greinar og fyrirtæki þar sem verðmætasköpunin byggist á tækni og þekkingu, frekar en hrávörum náttúrunnar.

Tölvunarfræðideildin ætlar sér hlutverk í að koma þessum hátækniiðnaði á flug - með útskrift nemenda, með því að ýta rannsóknum og þekkingu okkar út í atvinnulífið, en líka með beinni aðkomu og stuðningi við fyrirtæki á Íslandi sem byggja á þekkingu og hagnýtingu hátækni.

UTmessan.is

UTmessan 2017

Upplýsingatæknimessan var haldin í sjöunda sinn 3. og 4. febrúar 2017 í Hörpu í formi ráðstefnu og sýningar á föstudegi fyrir fagfólk í upplýsingatækni og sýningu sem var opin öllum á laugardegi. Upplýsingatækniverðlaun Ský voru einnig veitt á UTmessunni.

Hvað er UTmessan og fyrir hverja?

UTmessan er einn stærsti viðburður ársins í tölvugeiranum og hefur verið haldin árlega frá árinu 2011. Tilgangurinn er ekki síst til að sýna almenningi hversu stór og umfangsmikil þessi grein er orðin hér á landi. Á UTmessuna mæta öll helstu tölvu- og tæknifyrirtæki landsins og taka þátt með einum eða öðrum hætti og hvetja þannig fólk til að kynna sér um hvað tölvuiðnaðurinn snýst. Á UTmessunni sést fjölbreytileiki upplýsingatækninnar og þar sést svart á hvítu að allir hafa möguleika á að starfa í tölvugeiranum. Starfssviðið er bæði breitt og fjölbreytt og hentar bæði konum og körlum. Tilgangur UTmessunnar er að sjá aukin fjölda ungs fólks velja sér tölvugeirann sem framtíðarstarfsvettvang. Einnig viljum vekja áhuga almennings á upplýsingatækni og mikilvægi hennar á öllum sviðum daglegs lífs.

Að UTmessunni 2017 stóð Skýrslutæknifélagið í samstarfi við Háskólann í Reykjavík, Háskóla Íslands, og Samtök iðnaðarins með dyggum stuðningi Platinum styrktaraðilanna Sensa, Nýherja, Opinna kerfa og Gagnaveitu Reykjavíkur.

Yfir 1.000 manns voru á ráðstefnu UTmessunnar á föstudeginum og var það mál manna að gæði ráðstefnunnar hafi verið framar vonum. Yfir 50 fyrirlestrar voru í boði á 10 þemalínum ráðstefnunnar síðast en ekki síst með fróðlegum erlendum fyrirlestrum í Eldborg.

Um 13 þúsund manns mættu á opið hús á laugardeginum og hafa aldri komið jafnmargir á UTmessuna. Stemming var mjög góð að venju og ungir sem aldnir gengu um og fengu að sjá nýjustu tækni og vakti risavélmennið NOX athygli allra. Gestir fengu að prófa Hololens sem var í fyrsta sinn sýnt almenningi í heiminum. Tölvunördasafnið vakti einnig athygli og mátti sjá glampa í augum margra þegar þeir sáu gamla tölvuleiki og tölvuleikjatölvur á safninu. Hönnunarkeppni iðn- og vélaverkfræðinema HÍ laðaði marga að ásamt glæsilegu sýningarrými háskólanna í Norðurljósum og Silfurbergi. Mikið var um að vera í sýningarbásum fyrirtækjanna sem skörtuðu sínu fegursta á messunni. Gaman var að sjá fjölbreytileika gesta sem kíktu á UTmessuna þennan dag og það er óhætt að segja að UTmessan hefur stimplað sig inn hjá Íslendingum og lítur út fyrir að viðburðinn muni vaxa og dafna enn meira á næstu árum. Undirbúningur fyrir næstu UTmessu er farin af stað og er það von okkar að enn fleiri taki þátt í henni og við getum þannig sýnt Íslendingum hve mikill hugur er í fólki í tölvugeiranum.



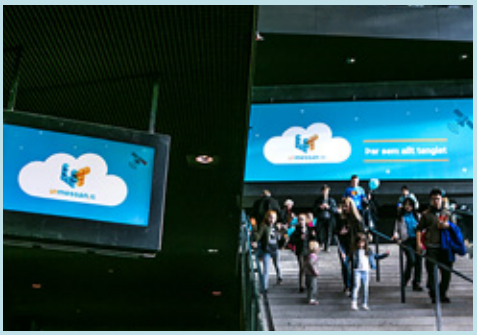

NÝHERJI





FORMULA STUDENT
101





TOLVUTEK





ský

FORRITUM NÝJA FRAMTÍÐ

Jóhanna Vigdís Guðmundsdóttir, framkvæmdastjóri Tengsla hjá Háskólanum í Reykjavík

Sú tækniþróun sem við höfum upplifað undanfarna tvo áratugi hefur verið svo hröð að oft er talað um fjórðu iðnbyltinguna, veldisvöxt og að við höfum bara rétt séð toppinn á ísjakanum. Það er ekki að ástæðulausu. Hraði tækninýjunganna veldur því að meirihluti þeirra starfa sem börnin okkar eiga eftir að sinna eru ekki enn orðin til. Áhrifin á atvinnulífið og samfélagið eru þegar umtalsverð, og munu verða meiri.

Öflug tölvutækni og gervigreind munu á næstu tuttugu árum sjálfvirknivæða allt að helming starfanna sem mannkynið vinnur í dag. Tæknimenntað fólk mun því ekki aðeins forrita nýjan hugbúnað heldur ný störf, nýja tegund atvinnulífs, nýtt samfélag og nýja framtíð.

Kynbundið náms- og starfsval er ennþá rótgróið í okkar samfélagi en ýmsar rannsóknir sýna að kynbundinn launamun megi að miklu leyti rekja til kynjaskiptingar starfa, þar sem hefðir og félagsmótun flokki störf hefðbundinna „karlastétta“ skör hærra en störf hefðbundinna „kvenna-stétta“. Rót kynbundins náms- og starfsvals má að mestu rekja til staðalmynda, hvort sem það er í nærumhverfinu, fjölmiðlum, sjónvarps-þáttum, eða minnisblaði unga mannsins sem starfaði hjá Google.

Í könnun sem Gallup gerði fyrir Google í Bandaríkjunum fyrir nokkrum árum kom fram að talsvert meiri líkur væru á að tölvunarfræðingar í sjónvarpi og kvikmyndum væru með gleraugu heldur en að þeir væru kvenkyns; 55% voru með gleraugu og 15% voru konur. Staðalmyndir af kynjunum móta hugmyndir stelpna og stráka um það hvað þau eigi að læra, hvað þau geti unnið við, hvaða hæfileika þau hafi og hvað þau geti yfirleitt. Þessi samfélagslega félagsmótun segir stelpum að 15% kvenna séu tölvunarfræðingar,

Stærðfræði er grunnur alls tæknináms. Samkvæmt samantekt Adams Grant, prófessors við Wharton háskóla, hafa stelpur og strákar sömu hæfileika til að læra stærðfræði en Adam brást við minnisblaði unga mannsins hjá Google með því að taka saman nokkrar staðreyndir um eðlislægan mun á körlum og konum, sem byggja á samanburði ítarlegra vísindalegra rannsókna. Adam dregur fram því sem næst 4000 rannsóknir, sem sýna að strákar eru ekki betri í stærðfræði en stelpur. Stelpum gengur jafn vel og strákum í stærðfræði í grunnskóla en strákum fer að ganga betur en stelpum í gagnfræðaskóla, en það á við í þeim löndum þar sem sýnileiki kvenna í rannsóknum er lítill og staðalmyndir tengja vísindastörf eingöng við karla. Þá er, aftur samkvæmt samanburði vísindarannsókna, afskaplega lítill munur á konum og körlum þegar litið er til hæfileika, viðhorfa og getunnar til að framkvæma. (sjá grein Adams Grant; Differences between men and women are vastly exaggerated)

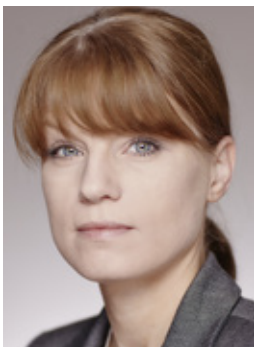
Snjóboltaáhrifin eru skýr; það er orðið almennt viðurkennt að við þurfum fleiri konur í tæknigreinar, fyrst til að velja sér nám í tæknigreinum í háskólum og síðan til að sækja um tæknistörf í fyrirtækjum. Þá er ekki síður mikilvægt að okkur hefur tekist að vekja fyrirtæki í tæknigreinum til vitundar um að blönduð teymi skila bestu vinnunni, það á jafnt við um stjórnir fyrirtækja, framkvæmdastjórnir og teymi sem vinna að tæknilausnum.

Við höfum tækifæri til að byggja upp öfluga atvinnugrein sem byggir á hugviti, þekkingariðnað með vel launuðum tæknistörfum, og getum gert þá atvinnugrein að undirstöðuatvinnugrein í íslensku samfélagi. Með því að fjölga konum í tækninámi og tæknigreinum er hægt að mæta alvarlegum skorti á tæknimenntuðu starfsfólki, sem hefur bókstaflega staðið í vegi fyrir vexti tæknifyrirtækja á Íslandi, um leið og við ráðumst að rótum þess hluta kynbundins launamunar sem orsakast af kynbundnu náms- og starfsvali.

Sú kynslóð stelpna og stráka sem nú er að vaxa úr grasi hefur stórkostlega spennandi tækifæri til þess að móta framtíðina, en við getum ekki sætt okkur við að nýtt samfélag og ný framtíð verði eingöngu mótuð á forsendum helmings mannkynsins. Það er nauðsynlegt að konur taki þátt í því að skapa samfélag framtíðarinnar. Þess vegna þurfum við fleiri konur í tölvunarfræði og tæknigreinar, þess vegna þurfum við Stelpur og tækni.

UPPLÝSINGAÖRYGGI Á TÍMUM BREYTINGA

Ragna María Sveinsdóttir, upplýsingaöryggissérfræðingur (Cyber, IT Security, Business continuity, Resilience, Sourcing, Fraud, Legal and Regulatory management)



Það er mikilvægt að einfalda viðfang og skilning fólks þegar kemur að upplýsingum á upplýsingaöld sem þessari. Þetta er kjarni málsins þegar fjallað er um upplýsingaöryggi. Þessi skilningur er ekki meðfæddur og skal það ekki tekið sem sjálfsagður hlutur að hver og einn eigi eða þurfi á þessum skilningi að halda. Hins vegar kemur það í verkahring þeirra sem meðhöndla upplýsingar á einn eða annan hátt að öðlast þessa kunnáttu, sem felur í sér hvernig rétt sé að meðhöndla tiltekna tegund upplýsinga í þeim tilgangi að vernda þær frá illgjörnum tilgangi. Það er mikill misskilningur að „rétt“ meðhöndlun og verndum upplýsinga sé eingöngu ábyrgð þeirra sem starfa í tölvudeildum fyrirtækja eða hafa upplýsingaöryggi í starfsheiti sínu.

Rétt meðhöndlun í þessu samhengi stýrist af því hverjar upplýsingarnar eru og hversu mikilvægar þær eru í samhengi við þá notkun sem á sér stað. Þetta ábyrgðarhlutverk fellur í garð notenda; hvort sem talað er um almennt [starfs-] fólk sem býr til upplýsingarnar, notar þær eða kerfisfræðinga (af óskilgreindum toga).

KERFIS- OG UPPLÝSINGAÖRYGGIS SÉRFRÆÐINGAR

Að sama skapi er ekki síður mikilvægt fyrir kerfis- og upplýsingaöryggisfræðinga að vera í stakk búnir að greina hvernig best er að vernda upplýsingarnar, út frá því hversu mikilvægar þær eru stofnunum og einstaklingum sem kunna að hafa aðgang að þeim. Sömuleiðis þarf að vernda upplýsingarnar svo að þær komist ekki í hendur þeirra sem gætu misnotað þær á einhvern hátt, t.d. til fjársvika.

Oft skapast mikill misskilningur á milli þessara tveggja flokka, þ.e.a.s. þeirra sem búa til upplýsingar og nota þær og þeirra sem hafa það í sínum verkahring að vernda þær í tölvukerfum og víðari netkerfum.

HEFÐBUNDIN MEÐHÖNDLUN UPPLÝSINGA

Grunnmeðhöndlun upplýsinga hefur hinsvegar ekki breyst svo mikið að það valdi okkur sem meðhöndlum þær erfiðleikum þegar kemur að skilningi okkar á mikilvægi þeirra í okkar vinnu. En það getur vafist fyrir þeim einstaklingum sem eru síður tæknivæddir og gera sér ekki grein fyrir líklegum hættum sem upplýsingum stafar af í nútíma samfélagi. Ætluð notkun upplýsinga hefur hins vegar aldrei fyrr verið eins víðtæk og breytileg sem og nú, með tilkomu stórra gagnasafna, skýjum af ýmsum toga, vélrænu námi, gervigreind, tækni og nýsköpun af ýmsum toga og ýmissa nýs búnaðar í persónulegri tækni á borð við tölvuúra o.s.frv.

Upplýsingar „fljóta“ alstaðar um og margfaldast á degi hverjum. Hraði margföldunar eykst að sama skapi með hverjum deginum. Á áhugi illræmdra einstaklinga vex á sama hraða, ef ekki hraðar. Erfiðara verður að vernda upplýsingar þegar kemur að nýrri tækni og breyttri hegðun notenda við upptöku nýrrar tækni. Í því samhengi má einnig nefna persónulega notkun snjallsíma, tölvuúra, spjaldtölva, nettengdra ísskápa, bíla o.s.frv. Listinn er óendanlegur, ef meðtalin er sú tækni sem notuð er í faggeirum fyrirtækja.

TRAUST OG ÞEKKING

Hluti af vandanum við að vernda upplýsingar felst í vanþekkingu og notkun á úreldum stöðlum og aðferðum við upplýsingavernd. Ásamt því að taka ekki til greina fyrirrætlanir fyrirtækja við notkun og vistum upplýsinganna. Ekki er lengur hægt að vanrækja þá þekkingu, reynslu og kunnáttu sem þarf til að vernda upplýsingar. Enn fremur má ekki gleyma því að verndun upplýsinga byggist á ýmsum stöðlum, s.s ISO27XXXX, SOC 1/2/3 og fleirum, því oftar en ekki, þrátt fyrir réttu umfangi og beitingu þeirra – er ósennilegt að þeir nái að réttri túlkun við innleiðingu.

Upplýsingaöryggi verður, sem fyrr segir, að mótast af ætlaðri notkun fyrirtækja og einstaklinga á upplýsingunum og hugsanlegri hættu sem stafar af misnotkun þeirra. Einnig þarf að taka mið af þeirri tæknikunnáttu sem hefur ekki talist nauðsynleg fram að þessu. Ekki má gleyma því flækjustigi sem felst í því að gangast við kröfum laga eða reglugerðar [svo dæmi séu tekin] á borð við komandi ESB reglugerð (nr. 2016/679 - GDPR[1]), sem fjallar sérstaklega um persónuvernd og rétt einstaklinga við almenna meðhöndum persónuupplýsinga. Það hefur ætíð fallið í hendur upplýsingaöryggissérfræðinga að finna tæknileg ráð og stillingar í tölvukerfum sem uppfylla kröfur slíkra reglugerða, og oftar en ekki er sennilegt að slíkar kröfur brjóti í bága við ætlaða notkun fyrirtækja á sömu upplýsingum.

NOTKUN OG NÚTÍMA TÆKNI

Fyrirtæki af ýmsum toga fjárfesta þessa dagana í tækni sem ætlað er að aðstoða við greiningu á hegðun og þörfum viðskiptavina. Umfram flest, með það að leiðarljósi að greina leiðir til að auka viðskiptin. Þessi stefna felur í sér notkun mikilla upplýsinga sem getur að líkindum auðkennt einstaklinga eða háttsemi þeirra og getur í sumum tilfellum stefnu fyrirtækja. Hvort um sig má telja til viðkvæmra upplýsinga sem hægt er að misnota, svo og bresti í öryggi ef þær komast í hendur rangra aðila.

Hér má einnig fjalla um þann mátt þeirra sem vilja ná yfirtökum á stýribúnaði tækja, með þeirri áætlun að valda fyrirtæki eða einstaklingum skaða. Tekið skal fram að þessi staðreynd á ekki eingöngu við um „erlend“ fyrirtæki – heldur líka um Íslensk fyrirtæki. Vanrækt á upplýsingavernd slíkra upplýsinga getur í flestum Evrópulöndum haft í för með sér háar sektir, svo ekki sé minnst á minnkandi orðstír fyrirtækja sem verða fyrir brotunum. Í alvarlegum tilfellum má jafnvel gera ráð fyrir mannskaða.

NÝ TÆKNI Í SAMHENGI UPPLÝSINGAÖRYGGIS

Tækni á borð við ský, vélrænt nám (e. machine learning), gervigreind og vélrænni lífkennagreiningu er ekki ný af nálinni. Aukin notkun þessarar tækni færir upplýsingaöryggissérfræðingum svefnlausar nætur. Hér er átt við upplýsingar sem geymdar eru í „opinberu“ skýi sem stjórnað er af gervigreind, þar sem umsjón og aðgengi að upplýsingum er að flestu leyti í höndum þriðja eða jafnvel fjórða aðila, þ.e. annarra en starfsmanna fyrirtækjanna þar sem upplýsingarnar eiga uppruna sinn. Í þessu samhengi er ekki hægt að verða sér úti um núverandi staðla og ætla sér að greina

og ráða fram úr hvernig best sé að vernda þær upplýsingar sem vistaðar eru í tilteknu tækniumhverfi.

Fyrir þessu eru ýmsar ástæður. Blanda af mismundandi tækni, breytt notkun upplýsinga, þær mörgu „hendur“ sem koma að umsjón mismunandi tækniumhverfa, nauðsynleg lög eða reglugerðir og líftími upplýsinga innan viðkomandi tækniumhverfis bæta frekar á flækjustig viðfangs sem upplýsingarnar eru vistaðar innan. Þar af leiðandi eru lagðar nýjar og frekar flóknar kröfur til notenda upplýsinganna, sem og á upplýsingaöryggissérfræðinga um að ná framgangi verndunar frá upphafi til enda. Þetta getur falið í sér verndun upplýsinga allt frá uppruna þeirra, sem oft má rekja til pappírsforms.

NÝ TÆKIFÆRI

Ísland er afar vel í stakk búið að staðsetja nýja leiðir í upplýsingaöryggi. Einkum og sér í lagi vegna þess hversu lítil þjóðin er og vegna hátta landans. Þá er átt við þær staðreyndir að Íslendingar hafa oft fleiri en eitt starfshlutverk vegna fólksfæðar. Erlendis þekkist frekar að eitt vel skilgreint starfshlutverk fellur eingöngu undir ábyrgðasvið eins starfsmanns/-konu. Mikilvægt er að skilgreina frekar að hér er eingöngu átt við einstaklinga sem vinna til dæmis sem kerfisstjórar með aukna þekkingu á verndun upplýsingakerfa. Fullgilding á öryggisstillingum kerfa væri hinsvegar framkvæmt af sjálfvirku kerfi og/eða sjálfstæðum einstaklingum með viðeigandi og dýpri þekkingu á málefninu, svo ekki stafi hætta á misferli.

Einfaldast og áhrifamest væri að sjá til þess að upplýsingatækni verði ekki sér fag eins og sést nú í öðrum löndum, heldur væri nær að sjá til þess að verndun upplýsinga verði hluti af hvers starfi einstaklings – hvað svo sem formlegt starfsheiti þess einstaklings ku vera.

Ragna María er menntuð í upplýsingaöryggi (MSc in IT security engineering) frá Bretlandi og býr yfir margra ára reynslu í faginu. Síðustu tæp 10 ár hefur hún búið erlendis og hefur á þeim tíma unnið við að vernda stærstu fyrirtæki heims í geirum; fjármála, olíu og gasiðnað – undir málefnum upplýsingaöryggis eða fjársvika.

Allar upplýsingar í greininni byggja á hennar persónulegu reynslu og skoðun, og vísar á engan hátt til hegðunar, stefnu eða skoðana þeirra fyrirtækja sem hún hefur starfar fyrir, né á engan hátt þess sem hún starfar hjá í dag.

HEIMILD

[1] https://www.personuvernd.is/ny-personuverndarloggjof-2018/leidbeiningar-fra-29.-gr.-vinnuhopi-esb/

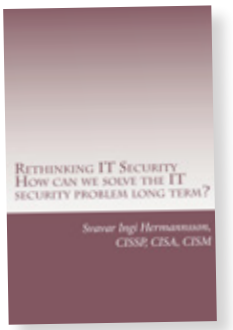
VIÐTAL VIÐ HÖFUND BÓKARINNAR:

RETHINKING IT SECURITY

HOW CAN WE SOLVE THE IT SECURITY PROBLEM LONG TERM?

Viðtal við Svavar Inga Hermannsson
Viðtalið tók Sigurjón Ólafsson

Svavar Ingi Hermannsson er einn fremsti sérfræðingur landsins í upplýsingaöryggi. Hann hefur sérhæft sig í upplýsingaöryggi og hugbúnaðarþróun undanfarna tvo áratugi. Svavar Ingi var formaður faghóps um öryggismál hjá Skýrslutæknifélaginu frá 2007 til 2012. Hann heldur reglulega fyrirlestra tengda upplýsingaöryggi á ráðstefnum bæði á Íslandi sem og erlendis og hefur meðal annars haldið fyrirlestra í Bretlandi, Þýskalandi, Úkraínu, Svíþjóð og Bandaríkjunum.



Í júní á þessu ári gaf hann út bókina Rethinking IT Security. How can we solve the IT security problem long term?. Við ákváðum að spyrja hann nokkra spurninga í tengslum við bókina.

HVER VAR HVATINN AÐ ÞVÍ AÐ SKRIFA ÞESSA BÓK?

Við erum í alvarlegum vandræðum í dag með tilliti til þekkingar á upplýsingaöryggi. Þetta á ekki bara við um Ísland heldur einnig um flest önnur lönd. Tillögurnar sem ég sting upp á í bókinni gætu mögulega bjargað okkur, ef brugðist er nógu skjótt við.

ER BÓKIN TÆKNILEG?

Ég reyndi að skrifa bókina eins ótæknilega og ég gat. Markmiðið er að ná til fólks sem er ótæknilegt. Ég tel að öllum geti þótt bókin athyglisverð. Ég vil að sjálfsögðu ná til allra, en helsti markhópurinn eru stjórnmálamenn og leiðtogar í menntamálum sem geta mögulega haft áhrif á stefnu landa, héraða og skóla.

UM HVAÐ FJALLAR BÓKIN?

Bókin útskýrir mikilvægi þess að auka þjálfun og kennslu í upplýsingaöryggi, sérstaklega fyrir þá sem eru ekki í tæknigreinaum en þó þarf vissulega einnig að bæta hana fyrir tæknigeirann í heild.

HVERJAR ERU HELSTU ÁSKORANIRNAR VIÐ AÐ INNLEIÐA TILLÖGURNAR ÞÍNAR?

Þetta eru mjög róttækar tillögur sem snúa að því að innleiða þjálfun tengda upplýsingaöryggi á öllum menntastigum og inn í flestar greinar eins og það á við hverju sinni. Þetta snýr að því að þjálfa kennara og uppfæra kennsluefni. Ef ákveðið væri að útfæra allar þessar hugmyndir þá má gera ráð fyrir því að það myndi krefjast mikilla fjármuna til að byrja með og mikillar vinnu. Ég tel að ávinningurinn sé þess virði en þetta er gífurlega stórt verkefni.

HVER HAFA VIÐBRÖGÐIN VERIÐ?

Viðbrögðin hafa verið mjög góð. Ég hef fengið fjölda spurninga í tengslum við efni bókarinnar, sem mér hefur þótt gaman að svara. Ég var t.d. beðinn um að halda fyrirlestur um efni bókarinnar á ráðstefnu í Belfast í September á þessu ári. Hægt er að nálgast upptöku af fyrirlestrinum á vefsíðunni minni: http://www.security.is/

RÉTT VIÐBRAGÐ MIKILVÆGT VEGNA ÖRT VAXANDI TÆKNILEGRAR ÓGNAR

Ólafur Róbert Rafnsson, ráðgjafi (partner) við áhættustjórnun og upplýsingaöryggi hjá Formönnum.

Mikil fjölgun upplýsingatækniógna hefur orðið og hefur mikil aukning verið á hnitmiðuðum árásum í þeim tilgangi að komast yfir aðgang og/eða upplýsingar í ýmsum tilgangi. Til dæmis getur vírussmit valdið miklum skaða og það er mjög mikilvægt að innleiða viðeigandi ráðstafanir til að lágmarka áhættu af völdum tölvuóværu af þessu tagi. Það er til dæmis hægt með því að vera með vírusvarnarhugbúnað og að uppsetning kerfishögunar sé með þeim hætti að auðvelt sé að bregðast skjótt við ef vart verður við tölvuinnbrot eða tölvuóværu til að lágmarka skaðann af slíku.

Það er því miður ekki til nein leið sem tryggir upplýsingavernd og/eða öryggi. Þess vegna er mjög mikilvægt er að vera með vel æfða og skilgreinda áætlun um viðbrögð til þess að stjórnendur og starfsmenn geti verið betur á verði gagnvart þessari ört vaxandi ógn. Mikilvægt er að bregðast rétt við ef vart verður við tölvuinnbrot eða tölvuóværu. Með vel skilgreindu verklagi eru fyrirtæki og stofnanir betur undirbúin fyrir slíkar ógnir, kerfisrof og/eða upplýsinga- og öryggisatvik.

Jafnvel með vírusvörn og fullkomum öryggiskerfum getur komið til vírussmits eða tölvuinnbrots, og þess vegna þurfa viðbrögð að vera vel grundvölluð og undirbúin. Í sumum tilfellum geta röng viðbrögð, til dæmis að uppræta tölvuóværu, skaðað verulega rannsóknarhagsmuni, s.s. í tilfelli sakamála og ef mikilvægt er að finna út hvað hafi gerst. Í slíkum tilvikum eru upplýsingar eins og kerfisdagbækur (e. logs) og réttir tímastimplar mikilvægustu upplýsingarnar, en þessi gögn eru yfirleitt ekki mikið notuð og stundum eru þau jafnvel ekki til. Því eru rétt viðbrögð gífurlega mikilvæg. Í sumum tilfellum er æskilegt að kalla til sérfræðinga áður en ráðist er í aðgerðir.

Fyrsta skrefið er yfirleitt að meta aðstæður og er mjög mikilvægt að bregðast rétt við því sum kerfi geyma ekki kerfisdagbækur lengur en í nokkrar klukkustundir og eru þá oft gögn ekki til þegar grípa þarf til þeirra. Þá skiptir máli að vera með vel útfært og æft viðbragð til að lámarka mögulegan þegar orðinn skaða. Mikilvægt er að skjala allt ferlið svo hægt sé að meta áhrif einnig ef til þess kemur að það þurfi að kæra til lögreglu.

BERA KENNSL Á SMIT

Að bera kennsl á hvaða kerfi eru smituð er ávallt fyrsta skref. Miðað við fjölbreytni upplýsingakerfa getur það reynst flókið. Hér eru nokkrar leiðir sem hægt er að hafa í huga sem geta hjálpað til:

- Setja í gang vírusskönnun á öllum þeim búnaði sem líklegt þykir að hafi smitast. Það gæti þurft að notast við fleiri en eina tegund vírusvarnarhugbúnaðar til að tryggja að tölvuóværa finnist, þó getur í sumum tilvikum verið óæskilegt að gagnsetja vírushreinsun ef slíkt getur t.d. eytt mikilvægum sönnunargögnum.
- Fara yfir kerfisdagbækur í eldveggjum og netbeinum.
- Koma leiðbeiningum áleiðis til starfsmanna um hvernig skal bera kennsl á möguleg vírussmit.
- Nota hugbúnað sem getur lesið IP pakka (e. packet sniffing tools) til að skoða með hvaða hætti tölvuóværan hagar sér á netkerfi.

TAKMÖRKUN Á SKAÐA VEGNA TÖLVUINNBROTS

Ef grunur er á að tölvuinnbrot sé að ræða þarf að haga viðbrögðum í samræmi við eftirfarandi:

HEMJA ÚTBREIÐSLU

Að hemja frekari útbreiðslu er hægt að framkvæma á margvíslegan máta. Hér eru nokkur dæmi;

- Nota þar til gerðan hugbúnað eins og IDS, AntiVirus o.s.frv. til að hafa hemil á útbreiðslunni.
- Með því að loka á netkerfi eins og Internet og innra net. Í sumum tilfellum gæti verið gott að aftengja öll kerfi frá miðlægum búnaði á meðan verið er að komast fyrir vandann.
- Með því að stöðva netþjónustu eins og sameiginleg netdrif (e. network share). Að loka fyrir slíkar þjónustur tímabundið getur verið auðveldara að halda frekari útbreiðslu í skefjum.
- Útrýma veikleikum stýrikerfa og eða annars búnaðar með því að tryggja að búið er að uppfæra með nýjustu öryggisplástrum (e. patching) frá framleiðanda.
- Virk þátttaka starfsmanna er mikilvæg sérstaklega ef ekki er hægt að fá aðstoð utan að.
- Að takmarka réttindi starfsmanna á eigin tölvum. Aukin réttindi á tölvum geta gert smit enn verra en það þarf að vera.
- Að virkja eldveggi á tölvum starfsmanna. Í einhverjum tilvikum hafa þeir eldveggir verið gerðir óvirkir, en það getur fjölgað smitleiðum.
- Hóp stillingar (e. group policy) ætti að stilla þannig að hægt sé takmarka aðgang og umgang um netkerfi. Einnig ættu starfsmenn að þekkja hvernig hægt er að takmarka aðgang ef til þess kemur.
- Net fyrirtækis ætti að brjóta upp í smærri net (e. subnet), en það getur aðstoðað við takmörkun ef til smits kemur.

Það er mikilvægt að skjala vel allar aðgerðir ef það er vel gert þá getur það hjálpað til við að einangra útbreiðsluna og hemja hana.

UPPRÆTA / HREINSA

Hreinsun skal framkvæma með það að markmiði að uppræta tölvuóværa að öllu leiti. Oftast dugar að notast við hefðbundin vírusvarnartól en í sumum tilfellum gæti þurft að setja búnað upp frá grunni. Ef tölvuóværa hefur komið fyrir bakhurð (e. backdoor) þá er ekki hægt að tryggja öryggi búnaðar að fullu nema með því að setja búnað upp frá grunni.

ENDURHEIMT

Markmiðið með öllum aðgerðum sem lýst er hér að ofan er að endurheimta kerfi, gögn og koma á stöðugleika á ný. Að endurheimta gögn og kerfi er líklegast gert í skrefinu hér á undan en það er einnig mikilvægt að ganga frá öllum breytingum á upplýsingakerfum sem gerðar voru til að meðhöndla ástandið. Þá er átt við að aftengja búnað, netdrif o.þ.h. sem notað var við hreinsunina. Áður en ferlinu líkur er mikilvægt að framkvæma áhættugreiningu til að tryggja að búið sé að komast fyrir vandamálið. Að lokum er mikilvægt að tilkynna öllum þeim sem taka þátt í að hemja útbreiðsluna og öðrum sem kunna að þurfa upplýsingar um stöðu mála.

SKÝJAGLEYPIR - FINGRAFÖR Í SKÝINU

Theódór Ragnar Gíslason, tæknistjóri hjá Syndis og sérfræðingur í tölvuöryggi

Notkun á skýjalausnum (SaaS) fer ört vaxandi[1] og með þeim mikla vexti skapast tækifæri en einnig nýjar áhættur. Undanfarin ár höfum við hjá Syndis unnið að rannsóknarverkefni sem ber heitið Skýjagleypir. Verkefnið snýst um þá staðreynd að fyrirtæki og fólk skilja eftir sig áhugaverð gögn í skýinu án þess að verða þess vör eða átta sig fyllilega á hvaða áhrif það getur haft. Tilgangur verkefnisins er að afla gagna og meta áhrif úr opnum efnisveitum og tengja gögnin saman. Þessi grein fjallar um að vekja upp vitund um þessa hættu og auka meðvitund um mögulegar ógnir í skýinu.

Flest fólk er meðvitað um þann fórnarkostnað sem fylgir notkun samfélagsmiðla þar sem við erum í raun að deila viðkvæmum persónuupplýsingum með erlendum stórfyrirtækjum. Við erum söluvaran þar sem okkar áhugamál eða jafnvel skoðanir eru notaðar til að senda okkur “hnitmiðaðar” auglýsingar. Ekki er eingöngu átt við stórfyrirtækin í þessu samhengi því þær viðbætur sem fólk bætir við sitt Facebook svo dæmi sé nefnt, getur verið að safna upplýsingum um þig eða þína vini. Margir eru meðvitaðir um þennan fórnarkostnað en skildi þetta einungis eiga við um hefðbundna samfélagsmiðla eins og Facebook eða Google?

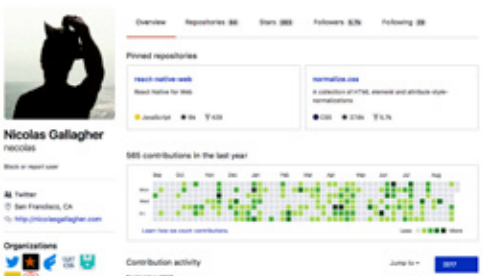
SAMFÉLAGSNET FORRITARA

Frumgerð Skýjagleypis safnar ítarlegum upplýsingum frá skýjaþjónustu og efnisveitu sem ber nafnið GitHub [2]. GitHub er notað af fyrirtækjum og einstaklingum um allan heim, aðallega forriturum, til að deila frumkóða, upplýsingum og gögnum. Allt er þetta gert í gegnum þessa skýjaþjónustu og að miklu leyti eru þetta opinberar upplýsingar sem allir geta sótt án mikillar fyrirhafnar. Að auki eru allar breytingar vistaðar og aðgengilegar með þægilegu móti. GitHub er jafnframt ört vaxandi [3] þjónusta sem telur nú yfir 20 milljón virkra notenda.

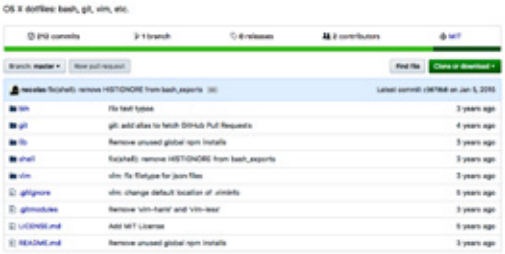
Þó GitHub sem slíkt er aðeins kerfi í kringum útgáfustýringu á hugbúnaði, þá hefur þróast samfélagsnet í kringum þessa tilteknu efnisveitu sem forritarar nota fyrir sín verkefni og einnig sem einskonar atvinnuumsókn. Fyrirtæki nota einnig GitHub til að efla þróun á þeirra innri lausnum. Ekki hefur verið birt hversu mikið af gögnum eru geymd á GitHub en ljóst er að um gríðarlegt magn að ræða og þau gögn sem þar má finna skilja eftir sig áhugaverð fingraför.

HVAÐA FINGRAFÖR SKILUR ÞÚ EFTIR?

Ef skoðað er handahófskennd síða einstaklings á GitHub má lesa ýmislegt um hann eins og mynd 1 sýnir. Sjá má hluti eins og fullt nafn (Nicolas Gallagher), hvar aðilinn býr, hvar hann vinnur (Twitter), hvaða vini hann hefur og hverjum hann fylgist með. Í sjálfu sér er þetta ekkert ólíkt því sem við deilum á hefðbundnum samfélagsmiðlum eins og Facebook og LinkedIn. Ef grannt er skoðað má sjá að þessi aðili er mjög virkur á GitHub og deilir einnig sínum eigin forritum og gögnum í kóðageymslum (e. repositories).



Með því að skoða eina slíka geymslu (e. dotfiles) á mynd 2 þá samanstendur hún af skráarsvæði þar sem aðilinn geymir stillingarskrár fyrir það stýrikerfi og hugbúnað sem hann notar. Óháð þessari tilteknu geymslu má einnig lesa ýmislegt eingöngu með því að horfa á innihald geymslunnar. Allar breytingar og viðbætur eru skráðar í atburðaskráningu og með því er hægt að sjá sögu geymslunnar frá því hún var stofnuð sem og innihald hennar frá fyrri tíð.



Með því að greina tegundir (e. extensions) skráa á mynd 2 má sjá að um er að ræða aðila sem notar MacOS stýrikerfi. Þetta í sjálfu sér er ekki geimvísindi en ef tekið er tillit til innihalds skráa, þá er fljótlega hægt að átta sig á hvaða hugbúnað aðilinn notar og jafnvel hvaða stillingar eru notaðar í þeim hugbúnaði og á stýrikerfinu. Þessi fingraför safnast svo saman þar til ágætis yfirsýn (e. profile) fæst yfir aðilann þar sem hægt er að segja með ákveðinni vissu ekki bara hvaða stýrikerfi aðilinn notar heldur einnig hvernig aðilinn ber sig að við sín daglegu störf. Það má til dæmis sjá í þessu tilfelli að hann er búinn að deila þeim stillingum sem hann notar á stýrikerfi sínu.

Með því að líta í gegnum atburðarskráningu á kóðageymslum þessa einstaklinga á mynd 3 fást enn meiri upplýsingar sem auka innsýn. Með þeim upplýsingum er hægt að átta sig á hegðunarmynstri, tengslaneti, og samhliða því nálgast öll póstföng sem aðilinn hefur notað til að vista breytingar á geymslum í hans eigu. Hægt er að átta sig á tæknilegum áhugamálum forritara (e. technical preferences) og þá til hvaða áhrifavalda aðilinn lítur upp til. Þó þessar upplýsingar virðist ekki mikilvægar við fyrstu sýn þá er slík innsýn gulls ígildi í augum tölvuglæpamanna og mætti jafnvel ætla að slíkar upplýsingar hefðu virði í markaðslegum tilgangi við þá sem vilja höfða til aðila sem hafa tiltekin tæknileg áhugamál.

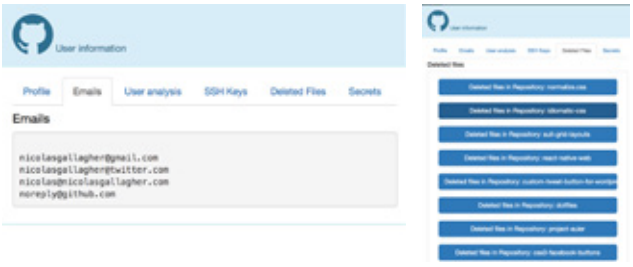
ÖFLUN UPPLÝSINGA MEÐ FORRITSVIÐMÓTI GITHUB

Sú hugmynd kviknaði að hægt væri að safna þessum upplýsingum fyrir alla notendur kerfisins og tengja gögnin saman. Fyrir Skýjagleypi, þá er notast við forritsviðmót (e. API) GitHub sem boðið er upp á til þess að einfalda upplýsingaöflun og fyrir GitHub var slíkt notað til að safna gögnum um alla notendur kerfisins. Tilgangurinn var að geta auðveldlega fundið upplýsingar um alla notendur kerfisins, hvort sem um fyrirtæki eða einstakling væri að ræða. Ákveðið var að skilgreina einstaklinga og fyrirtæki sem nóður sem gætu mögulega tengst saman.

Eftir slíka skilgreiningu þá er hægt að keyra kerfið á tiltekið fyrirtæki og ítra í gegnum allar kóða geymslur sem tilheyrir viðkomandi því. Með því að ítra í gegnum alla atburðaskráningu er hægt að finna alla aðila sem höfðu gert breytingar á geymslum í eigu fyrirtækisins. Sama ferli er síðan endurtekið fyrir alla þá einstaklinga sem komu fram í atburðaskráningu. Með þessu er hægt að finna flesta raunverulegu starfsmenn fyrirtækis, þó þeir komi alls ekki allir fram á GitHub síðu fyrirtækja. Fyrir þessa grein var ákveðið af handahófi að velja Twitter til að sýna fram á þessa hugmynd og þá útfærslu sem valin var fyrir þetta verkefni.

Eins og má sjá á niðurstöðum á mynd 4 voru aðeins 27 skráðir starfsmenn samkvæmt GitHub síðu Twitter en eftir keyrslu á Skýjagleypi er búið að finna 130 starfsmenn eingöngu með því að ítra í gegnum atburðaskráningu á geymslum í eigu fyrirtækisins.

Eftir keyrslu á Skýjagleypi þar sem öll gögn sem tengjast Twitter og mögulegum starfsmönnum, voru sótt var útkoman 132GB og inniheldur það gagnasafn alla atburðarskráningu á öllum kóðageymslum Twitter sem og þeirra sem kerfið skilgreinir sem starfsmenn. Ef við snúum okkur aftur að honum Nicolas Gallagher þá má til dæmis sjá á mynd 5 tölvupóstföng hans og einnig skrár sem hann hefur eytt úr sínum kóða geymslum.



Aðrar upplýsingar eins og greiningu á notandanum eru ekki birtar í þessari grein og eru háð þeim leitarskilyrðum sem eru sett, en fyrir samantekt á þeim gögnum sem tengdust þessum tiltekna notanda samanstendur það af eftirfarandi:

1. Alls 49MB af gögnum frá Nicolas
2. Alls 3634 skrár
3. Alls 30 mismunandi skráarendingar (File extensions)

LEYNDARMÁLIN ERU EKKI AFMÁÐ AUÐVELDLEGA

Forritarar er áhugaverður hópur fyrir þá sem vinna við öryggismál og einnig í hugum tölvuglæpamanna. Þetta eru aðilarnir sem skrifa hugbúnaðinn sem keyrir í raunumhverfi og hafa því óbeint gríðarlega mikil völd og aðgang. Þetta gerir það að verkum gögn forritara geta verið viðkvæm sem þýðir að þeir eru áhugaverð skotmörk fyrir tölvuárásir. Það eru einnig þekkt tilvik þar sem forritarar hafa ómeðvitað sett inn viðkvæm leyndarmál eins og dulkóðunarlykla [4] eða jafnvel notendanöfn og lykilorð þeirra að viðkvæmum kerfum og gagnagrunnum. Allt eru þetta upplýsingar sem geta verið til staðar í þeim kóðageymslum sem einstaklingar og fyrirtæki setja inn á GitHub.

Stundum átta aðilar sig á mistökum sínum og gera breytingu á sinni kóðageymslu til að eyða t.d. lykilorði eða dulkóðunarlykli en eðli GitHub er þannig að allt er skráð og því eru þessar upplýsingar enn aðgengilegar. Til eru þó nokkur kerfi sem afla þessara gagna en með Skýjagleypi var ráðgert að útbúa einfalda leitarvél að þessum gögnum svo mætti auðveldlega þefa uppi slík leyndarmál. Í ljós hefur komið að API lyklar, notendanöfn og lykilorð og margt annað er að finna í þessum kóðageymslum eða atburðaskráningu sem geymd er.

SÉRHÆFÐ TÖLVUÁRÁS SETT SAMAN MEÐ 0-DAY ÖRYGGISVEIKLEIKUM

Í einu verkefni hjá Syndis fyrir alþjóðlegt fyrirtæki var ákveðið að reyna að nota þau fingraför sem safnað hafði verið saman með Skýjagleypi. Fyrir þann sem vinnur við öryggismál er það eitt að vita hvaða hugbúnað viðkomandi aðili notar, mikið forskot og getur aukið líkur á árangri tölvuárása. Ástæðan er sú að hægt er að velja tól (e. exploit) sem notfærir sér þekkta veikleika í þeim hugbúnaði sem vitað er að notandi er með uppsettan. Að auki er hægt að notfæra sér þessar upplýsingar til þess að velja hugbúnað til að þessa að leita að öryggisvillum í og það er það sem við ákváðum að notfæra okkur í verkefni með þessu alþjóðlega fyrirtæki.

Við fundum veikleika í ýmsum hugbúnaði en fyrir valinu varð MacVim [5] og SourceTree [6] sem er hugbúnaður sem margir þróunaraðilar nota. Um er að ræða svokallað „Remote Code Execution“ veikleika en í gegnum slíkt er hægt að taka yfir tölvu einstaklings. Með því að notfæra okkur þær aðferðir sem Skýjagleypir bíður upp á, þá gátum við staðhæft að 30 starfsmenn væru að nota þennan tiltekna hugbúnað. Við vissum líka hvernig stillingarnar voru hjá nokkrum þeirra, þar sem þeir voru með sérhæfðar stillingar fyrir Safari vafrann, sem gerði það að verkum að við vissum að við gætum brotist inn á tölvurnar þeirra eingöngu með því að fá þessa starfsmenn til að smella á hlekk. Þetta er dæmi um 0-day [7] (núll-dags) tölvuárás með notkun „spear phishing“ [8] til þess að fá fólk til að smella á hlekk, t.d. í gegnum tölvupóst.

HEIMILDIR

[1] http://www.zdnet.com/article/saas-in-2016-the-key-trends/
[2] https://GitHub.com
[3] https://www.wired.com/2015/03/GitHub-conquered-google-microsoft-everyone-else/
[4] http://arstechnica.com/security/2015/03/in-major-goof-uber-stored-sensitive-database-key-on-public-GitHub-page/
[5] https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2017/february/technical-advisory-shell-injection-in-macvim-mvim-uri-handler/
[6] https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2017/february/technical-advisoryshell-injection-in-sourcetree/
[7] https://en.wikipedia.org/wiki/Zero-day(computing)
[8] https://en.wikipedia.org/wiki/Phishing#Spear_phishing

ÚTTEKT Á ÖRYGGI OPINBERRA VEFJA 2017

Svavar Ingi Hermannsson, sérfræðingur í upplýsingaöryggi og Guðbjörg Sigurðardóttir, skrifstofustjóri Samgöngu- og sveitarstjórnarráðuneytinu

Fyrsta heildarúttektin á gæðum opinberra vefja, Hvað er spunnið í opinbera vefi, var framkvæmd árið 2005 og hafa slíkar úttektir verið gerðar annað hvert ár upp frá því. Í tengslum við úttektina árið 2017 var í annað sinn gerð sérstök úttekt á öryggi opinberra vefja ríkis og sveitarfélaga. Markmiðið er að stuðla að auknu öryggi á opinberum vefjum og er unnið að því með því að afla upplýsinga um öryggi þeirra og koma ábendingum um hvað þurfi að lagfæra til ábyrgðarmanna og vefstjóra einstakra vefja. Í mörgum tilfellum er um að ræða atriði sem auðvelt er að ráða bót á þegar vitneskjan um þau liggur fyrir. Upplýsingar um öryggi einstakra vefja verða ekki birtar opinberlega, þær verða einungis aðgengilegar þeim sem vinna að úttektinni og forsvarsmanni/vefstjóra viðkomandi ráðuneytis, stofnunar eða sveitarfélags.

AÐFERÐIN

Vefirnir voru skannaðir með forritum sem leita að öryggisveikleikum. Þeir vefir sem taldir eru innihalda sérstaklega viðkvæmar upplýsingar voru skoðaðir ítarlegar, meðal annars með hliðsjón af þekktri aðferðafræði sem lýst er í Vefhandbókinni á vef stjórnarráðsins (m.t.t Open Web Application Security Project (OWASP) top 10 öryggisveikleikum) [1].

Ekki voru framkvæmdar innbrotsprófanir heldur einungis leitað eftir öryggisveikleikum. Sjá útskýringar á framkvæmd öryggisúttektarinnar á vef stjórnarráðsins [2].

Áður en framkvæmd verkefnisins hófst var sendur út tölvupóstur á ábyrgðaraðila opinberra vefja þar sem úttektin var útskýrð og óskað eftir því að ábyrgðaraðilarnir létu þjónustuaðila sína vita af fyrirhugaðri úttekt. Að auki var haldinn kynningarfundur fyrir ábyrgðaraðila og þjónustuaðila þar sem farið var yfir fyrirhugaða úttekt og spurningum svarað.

MAT Á VEIKLEIKUM

Mat á veikleikum er byggt á svokölluðum CVSS-gildum (e. Common Vulnerability Scoring System) þegar þau eru til. Ef þau eru ekki til er byggt á huglægu mati. Heildarmat á veikleikum vefs tekur mið af „veikasta hlekknum“ sem finnst á vefnum eða með öðrum orðum stærsta öryggisveikleikanum sem finnst. Flokkunin sem stuðst var við í þeim skýrslum sem ábyrgðaraðilar fá í hendur fylgdi eftirfarandi viðmiðum:

CVSS-gildi	Mat á veikleikum
7 - 10	Alvarlegir veikleikar
0.1 - 6.9	Veikleikar fundust
0	Ekki fundust veikleikar

FYRIRVARI

Hvort sem veikleikar fundust í öryggisúttektinni eða ekki, er alls ekki tryggt að öryggisveikleikar séu ekki til staðar. Öryggisúttekt sem þessi er bundin við umfang, tíma, útgáfu viðkomandi vefkerfis, vefmiðlara og stýrikerfi á þeim tíma og þeim aðgangi sem prófunaraðili hafði að vefnum. Það er mikilvægt að endurtaka öryggisúttektir reglulega, sérstaklega þegar meiriháttar breytingar eru gerðar á vefkerfi eða þegar nýrri virkni er bætt við eða breytt.

HELSTU ÁHÆTTUÞÆTTIR

Það er mikilvægt að taka fram að helstu áhættuþættirnir sem snúa að opinberum vefjum eru nákvæmlega sömu áhættuþættir og snúa almennt að vefjum fyrirtækja og einstaklinga. Þó svo að allar tegundir öryggisveikleika sem taldir eru upp í OWASP top 10 hafi fundist, þá eru samt sem áður sumir öryggisveikleikar sem eru líklegri til að vera til staðar en aðrir. Það eru helst tveir áhættuþættir sem þarf að huga að. Annars vegar er innsetning á öryggisuppfærslum (fyrir stýrikerfi, vefmiðlara, vefumsjónarkerfi og íhluti vefumsjónarkerfa) og hins vegar að tryggja að viðkvæmar upplýsingar (eins og t.d. notandanafn + lykilorð) séu send yfir dulkóðuð samskipti (HTTPS/TLS).

Í mörgum tilfellum eru áhættan fólgin í því að ábyrgðaraðilar vefja gefi sér rangar forsendur. Ábyrgðaraðilar vefja gætu ranglega gert ráð fyrir eftirfarandi þáttum án þess að það sé tekið fram í samningum:

- að hýsingaraðili muni sjá um að setja inn öryggisuppfærslur fyrir stýrikerfi, vefmiðlara, vefumsjónarkerfið og íhluti vefumsjónarkerfis.
- að framleiðandi vefumsjónarkerfis láti vita ef öryggisveikleikar finnast í viðkomandi útgáfu af vefumsjónarkerfi.
- að framleiðandi bjóða upp á öryggisuppfærslur á vefumsjónarkerfi kaupanda að kostnaðarlausu.
- að vefkerfi sé sett upp á öruggan hátt án þess að viðskiptavinur biðji um það sérstaklega.

Eftir að hafa aðstoðað fjölda opinberra aðila við að bregðast við þeim ábendingum sem komu úr öryggisúttektinni 2015 ákvað samgöngu- og sveitastjórnarráðuneytið (þá innanríkisráðuneytið) að gefa út drög að samningsviðauka vegna upplýsingaöryggis. Þessi drög er hægt að finna á vef stjórnarráðsins [3].

Samningsviðaukinn er átta blaðsíðna skjal sem hugsaður er sem samningsviðauki við núverandi samninga við þjónustuaðila, hýsingaraðila og hugbúnaðarhús sem opinberir aðilar eru nú þegar í viðskiptum við. Þar kemur meðal annars fram krafa á hýsingar- og þjónustuaðila að setja reglulega inn öryggisuppfærslur og að notast ekki við upplýsingakerfi þar sem framleiðandi er hættur að styðja við þau í formi öryggisuppfærslna.

TÆKIFÆRI FRAMUNDAN

Með tilliti til nýrra reglna og reglugerða (GDPR, NIS tilskipun, o.fl.) þar sem miklar sektir geta legið við broti gegn ákvæðum í nýju löggjöfinni (t.d. allt að 4% af ársveltu í tilfelli nýju persónuverndarreglugerðarinnar) eru mikil tækifæri fyrir hýsingaraðila, hugbúnaðarhús, þjónustuaðila, opinberaaðila og almenn fyrirtæki að huga að rekstraröryggismálum. Allir geta skoðað samningsviðaukann og tileinkað sér þær stýringar sem taldar eru upp þar auk þess að nota samningsviðaukann eða þætti úr honum í samningum sínum við birgja og aðra ytri aðila.

Eftirfarandi eru dæmi um stýringar sem koma fram í samningsviðaukanum:

- Öryggisstefna
- Áhættumat
- Formlegt ferli við stjórnun aðgangs
- Formlegt ferli við öryggisuppfærslur
- Formlegt ferli við veikleikagreiningar og innbrotsprófanir
- Innbrotsvöktunarkerfi
- Frávikaskráningar og tilkynning á öryggisatvikum
- Innra eftirlit
- O.fl.

HELSTU NIÐURSTÖÐUR

Það kemur ef til vill ekki á óvart að þeir opinberu aðilar sem hafa meira fjármagn, stærri tölvudeildir og eru að meðhöndla viðkvæmar upplýsingar eru líklegri til að hafa öryggismálin í lagi. Í fyrstu öryggisúttektinni 2015 fundust allar tegundir öryggisveikleika sem taldar eru upp í OWASP topp 10. Sumir vefir og þeirra umhverfi voru að því er virtist gallalaus en aðrir vefir og vefumhverfi virtust hafa verið sett upp fyrir áratug eða svo og ekki fengið viðhlítandi viðhald enda voru niðurstöðurnar fyrir þá vefi í samræmi við það.

Það er mikilvægt að hafa í huga að hverju upplýsingakerfi og hverju vefumsjónarkerfi sem ákveðið er að taka í rekstur fylgir ábyrgð á að fylgjast með öryggisuppfærslum og setja reglulega inn nýjustu öryggisuppfærslurnar frá framleiðanda. Þessu til viðbótar skiptir einnig miklu máli að horfa fram á við og þegar framleiðandi er búinn að gefa út yfirlýsingu um að hann ætli að hætta að styðja við viðkomandi útgáfu af stýrikerfi, vefmiðlara eða vefumsjónarkerfi þá þarf strax að huga að því hvernig bregðast eigi við, þó svo að í einhverjum tilfellum fái menn nokkurra ára fyrirvara. Ef öryggisuppfærslur eru settar upp jafnóðum og þær eru gefnar út og unnið er jafnt og þétt að öryggismálum er auðvelt að ná árangri. Ef hins vegar beðið er of lengi með uppfærslur þá safnast upp ákveðin tækniskuld sem getur leitt til þess að það verði of seint að bregðast við því tölvuinnbrot hafi þegar átt sér stað.

Það er ánægjulegt að viðbrögð ábyrgðaraðila opinberra vefja við niðurstöðum fyrstu úttektarinnar voru mjög jákvæð. Flestir brugðust fljótt og örugglega við ábendingunum og komu úrlausnarverkefnum í farveg auk þess sem margir nýttu sér tækifærið og fengu aðstoð frá ráðuneytinu við að greina niðurstöðurnar og meta hvernig væri best að bregðast við.

SLÓÐIR

[1] https://www.stjornarradid.is/verkefni/upplysingasamfelagid/opinberir-vefir/vefhandbokin/6.-oryggi/6.2-oryggi-veflausna/

[2] https://www.stjornarradid.is/verkefni/upplysingasamfelagid/opinberir-vefir/uttektir-a-opinberum-vefjum/

[3] https://www.stjornarradid.is/efst-a-baugi/frettir/stok-frett/2017/01/06/Upplysingaoryggi-samningsvidauki-leidbeiningar-og-eydublod-fyrir-gerd-ahaettumats/

BÖRN, SNJALLTÆKI OG SANNLÍKI

Ásdís Bergþórsdóttir, kerfisfræðingur og sálfræðingur

Mikið er rætt um börn og snjalltæki og til landsins hafa verið kallaðir erlendir sérfræðingar til að fræða okkur. Bugl fékk Gwenn S. O´Keeffe, barnalækni til landsins og á ráðstefnu Bugl vitnaði læknir mikið í geðlækninn Victoriu Dunckley. Félag foreldra leikskólabarna í Reykjavík fékk Chris Rowan iðjuþjálfa og Catherine Steiner-Adair sálfræðing á ráðstefnu sína. Engin þeirra hefur birt ritrýnda rannsókn á þessu sviði samkvæmt leit á *Google Scholar* og *Web of Science*. O'Keeffe[1,2] hefur birt greinar á þessu sviði byggðar á heimildum í ritrýndum fræðitímaritum. Steiner-Adair[3] hefur birt grein um tölvunotkun í almennu riti, en ekki í fræðiriti um skólamál. Hún vann reyndar við Harvard og var þá í rannsóknum á átröskunum[4]. Allar hafa þær gefið út bækur[5,6,7,8] sem fjalla um börn og tölvur/skjátæki og selja sérfræðiþjónustu á þessu sviði.[9,10,11,12] Þar sem engin þessara kvenna hefur birt rannsóknargreinar á þessu sviði er ljóst að fræðimennska þeirra byggist á notkun heimilda. Til þess að meta málflutning þeirra þarf því að skoða heimildameðferð þeirra. Hér verður skoðað heimildameðhöndlun þeirra skoðuð. Sökum plássleysis er aðeins hægt að taka örfá dæmi.

STEINER-ADAIR, SPONGEBOB OG WALL STREET JOURNAL

Steiner-Adair[3] vitnar í rannsókn og segir hana sýna fram á að aðeins 9 mínútna áhorf á SpongeBob geti leitt til ofbeldishegðunar. Rannsóknin sýndi að eftir að fjögurra ára börn horfðu á níu mínútur af SpongeBob, þætti ætluðum börnum 6-11 ára, fór þau að skorta athygli og áttu erfiðara með að bíða eftir umbun[13]. Hins vegar var ekkert minnst á agressífa hegðun eða ofbeldi í rannsóknargreininni.

Steiner-Adair[3] vitnar einnig í Wall Street Journal (WJS)[14]. Hún heldur því fram að í gegnum rannsóknir og viðtöl við sérfræðinga sé hægt að tengja aukna slysatíðni barna yngri en fimm ára við aukna notkun skjátækja, þar sem hinir fullorðnu séu svo uppteknir við þau. WSJ er fréttamiðill og viðtöl þess hafa ekki sama gildi og ritrýndar rannsóknir. Í grein WSJ er engar eiginlegar rannsóknir að finna heldur er því lýst að slysatíðni barna hafi aukist á sama tíma og snjallsímanotkun hafi aukist. Sú ályktun er dregin að aukin slysatíðni sé vegna minna eftirlits með snjallsímanotkun barna. Þetta er því kenning sem ekki er studd af neinum rannsóknum. Fullyrðing Steiner-Adair um að sýnt hafi verið fram á þetta stenst því ekki.

ROWAN OG PRÓSENTUR

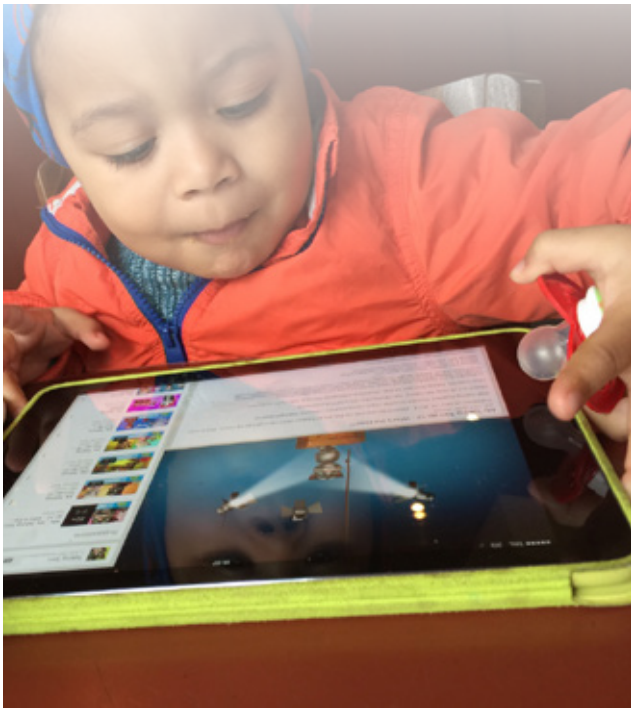
Rowan[15] tekur fram í glærum sínum að árið 2025 muni helmingur drengja verða á einhverfurófi. Hún virðist tengja aukningu einhverfu við aukningu á skjátíma barna. Þetta er sérstakt í ljósi þess að einhverfa er í langflestum tilfellum talin orsakast af erfðum[16]. Rowan er þarna að vitna í ummæli Stephanie Seneff,[17] doktors í rafmagnsverkfræði og tölvunarfræði við MIT. Seneff[18] álítur að aukning einhverfu sé vegna illgresiseyðisins glyfosat, öðru nafni RoundUp. Þessi ummæli um tíðni einhverfu lét hún falla á ráðstefnu en þessar tölur hafa ekki birst í fræðitímariti. Seneff hefur engan bakgrunn í faraldsfræði eða einhverfu og mér er ekki kunnugt um neinn fræðimann á sviðinu sem telur að þessar tölur standist. Rowan virðist velja heimildina vegna þess að tölurnar geta styrkt mál hennar en ekki af því að þær séu viðurkenndar af sérfræðingum. Það er ekki fræðimennska að tína upp vafasamar heimildir af því að það hentar rökstuðningnum. Rowan segir einnig að 42% tíu ára barna noti klám og minnist á hversu alvarleg klámnotkun barna er. Þegar heimildin19 er skoðuð kemur í ljós að 1% drengja og 2% stúlkna á aldrinum 10-11 ára sóttust eftir klámi á árstímabili. Hins vegar sáu 42% ungmenna á aldrinum 10-17 ára klám á árstímabili en 14% barna á þessum aldri voru að leita að klámi og voru því að nota það. Rowan er einfaldlega ekki með réttar tölur og flestum ætti að vera ljóst að það stenst ekki skoðun að 42% tíu ára barna noti klám.

DUNCKLEY OG HEILINN

Victoria Dunckley[20] telur að of mikill skjátími skaði heilann. Hún vitnar í margar rannsóknir um að tölvuleikjaspilun valdi óafturkræfum breytingum í heila. Vandamálið er að þessar rannsóknir eru fylgnirannsóknir. Þær svara því ekki hvort spilunin breyti einstaklingum með týpíska heilastarfsemi yfir í óvenjulega starfsemi eða hvort einstaklingar með óvenjulega heilastarfsemi sæki frekar í tölvuleiki. Til að kóróna allt virðist Dunckley telja að hægt sé að alhæfa fylgnirannsóknir á tölvuleikjum yfir á allan skjátíma sama hvers eðlis hann er og að allur rafrænn skjátími skaði heilann, sbr. heiti á pistli hennar Too much screen time damages the brain .

Dunckley[21] listar einnig margar ástæður þess að börn á einhverfurófinu séu viðkvæmari fyrir skjátíma og tæknifíkn. Þessar ástæður koma ekki frá fræðimönnum á sviði einhverfu heldur tekur Dunckley þær saman sjálf. Ein af ástæðum sem hún nefnir er sú að bólgur í miðtaugakerfi tengist einhverfu. Hún telur að skjánotkun valdi streitu, minnki framleiðslu á melantónín, geri svefn verri og að slíkt auki bólgurnar. Vandinn er sá að greinin sem hún vitnar í sýnir ekki fram á að einhverfa tengist bólgum í miðtaugakerfi heldur er þar sett fram kenning um á hvaða hátt einhverfa gæti tengst staðbundnum bólgum í heila (e. Focal Brain Inflammation)[22], en sú kenning er ekki viðurkennd af sérfræðingum. Engin rannsókn var framkvæmd í tengslum við greinina. Greinin[23] sem fjallar um tengsl aukinna bólgna og svefngæða fjallar svo um astma, iktsýki, lúpus og langvinna bólgusjúkdóma í þörmum en ekki um staðbundnar bólgur í heila. Það eru einfaldlega engar rannsóknir sem sýna fram á að skjánotkun valdi auknum bólgum í heila hjá einstaklingum á einhverfurófinu. Samt var vitnað í þetta á ráðstefnu Bugl.[24]

Á sama hátt segir Dunckley að einstaklingar á einhverfurófi geti verið viðkvæmari fyrir rafsegulbylgjum frá skjátækjum en aðrir. Greinin[25] sem hún vitnar í setur fram þá kenningu að rafsegulbylgjur geti haft áhrif á frumur og margvíslega starfsemi þeirra og mögulega valdið einhverfu. Þessi kenning er ekki viðurkennd af fræðimönnum á sviði einhverfu. Greinin sýnir ekki fram á nein tengsl einhverfueinkenna og rafsegulbylgna



og var engin rannsókn framkvæmd í tengslum við greinina. Samt er talin ástæða til að vitna í þessa skýringu á ráðstefnu Bugl[24].

O'KEEFFE OG ÖRUGG NETNOTKUN

O'Keeffe[26] tekur allt annan pól í hæðina en hinar þrjár. Hún einblínir á örugga notkun en ekki fíkn eða heilkenni. O'Keeffe notar heimildir aðallega til að sýna fram á hvað börn og ungmenni eru að gera á netinu. Fullyrðingar hennar eru hógværar. Hún segir að samfélagsmiðlar séu tæki og séu aðeins hættulegir ef þeir eru notaðir hættulega. Ég hef heldur ekki fundið nein dæmi um ranga eða vafasama meðhöndlun á heimildum hjá henni. Hún virðist til dæmis ekki nota fylgnirannsóknir til að sýna fram á orsakir. Hér virðist því vera allt önnur og betri vinnubrögð á ferðinni. Því er ljóst að hægt er að fara á ábyrgan hátt með heimildir í þessum málaflokki.

SANNLÍKI

Spurningin sem vaknar hjá mér eftir að hafa skoðað frumheimildir og heimildanotkun þriggja þessara kvenna er hversu mikið er að marka málflutning þeirra. Við lifum á upplýsingaöld en líka á öld sannlíkis (e. alternative truth). Hver sem er getur sett fram fullyrðingar og stundum verður til sannlíki á netinu – eitthvað sem auðvelt er að finna og fletta upp en á sér litla eða enga stoð í raunveruleikanum. Að vera með menntun á ákveðnu sviði þýðir ekki sjálfkrafa að viðkomandi fari rétt með heimildir. Þegar um er að ræða sérfræðinga sem tjá sig á vefnum eða í eigin bókum er enginn sem athugar heimildirnar. Vissulega eru til sérfræðingar eins og O'Keeffe sem stunda ábyrga meðhöndlun heimilda en það er bara alls ekki algilt að svo sé. Lesandinn þarf að skoða hvort eitthvað sé að marka fullyrðingarnar. Sé það ekki gert ferðast sannlíkið áfram. Eins og ég hef sýnt með dæmum þá enda sannlíki á ráðstefnum hérlendis og fara þaðan út í samfélagið þar sem það lifir væntanlega sjálfstæðu lífi óháð rannsóknum og fræðimennsku.

Lesendum er bent á að Tölvumál er ekki fræðitímarit og greinar eru ekki ritrýndar. Lesendur eru því hvattir til að kynna sér heimildir sem vísað er á í greininni til að meta sjálfir sannleiksgildi þess sem fram kemur. Höfundur hefur lagt mikla áherslur á að nota heimildir sem eru aðgengilegar og lesendur geta sannreynt. Hægt er að fara á síðuna notendur.hi.is/asb23/heimildir.html. Þar eru beinir tenglar á allt aðgengilegt efni sem vitnað er til.

(ENDNOTES)

1 O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. Pediatrics, 127(4), 800-804.
2 O'Keeffe, G. S. (2012). Overview:: New Media. Pediatric Clinics of North America, 59(3), 589-600.
3 Steiner-Adair, C. (2015). The Big Disconnect: Your Student in Class vs. Your Student Online. Independent School, 74(2), n2.
4 Sjostrom, L. A., & Steiner-Adair, C. (2005). Full of ourselves: A wellness program to advance girl power, health & leadership: An eating disorders prevention program that works. Journal of nutrition education and behavior, 37, S141-S144.
5 Steiner-Adair, C., & Barker, T. H. (2013). The big disconnect: Protecting childhood and family relationships in the digital age. Harper Business.
6 Dunckley, V. L. (2015). Reset Your Child's Brain: A Four-Week Plan to End Meltdowns, Raise Grades, and Boost Social Skills by Reversing the Effects of Electronic Screen-Time. New World Library.
7 O'Keeffe, G. S. (2005). CyberSafe. Elk Grove Village, IL: AAP Books, 247-9.
8 Rowan, C. (2010). Virtual Child: The terrifying truth about what technology is doing to children. Sunshine Coast Occupational Therapy Incorporated.
9 Pediatrics Now (e.d). Pediatrics Now. Sótt 13. maí 2017 af http://www.pediatricsnow.com/.
10 Steiner-Adair (e.d.). Catherine Steiner-Adair. Sótt 13. maí 2017 af http://catherinesteineradair.com/.
11 Dunckley, V.L. (e.d.). Victoria L. Duncley, M.D.. Sótt 13. maí 2017 af http://drdunckley.com/.
12 Zone in Workshops (e.d). Zone in Workshops. Sótt 13. maí 2017 af http://www.pediatricsnow.com/.
13 NBC Wasington (2011, 12. september). Study says SpongeBob bad for kid's mental function. Sótt 12. maí 2017 af http://www.nbcwashington.com/news/local/DC-Study-Says-SpongeBob-Bad-For-Kids-Mental-Function-129641993.html.
14 Worthen, B. (2012, 29. September) The Perils of Texting While Parenting. Wall Street Journal. Sótt 12. maí af 2017 https://www.wsj.com/articles/SB10000872396390444772404577589683644202996.
15 Rowan, C. (e.d.). Mixed Signals. Sótt 15. maí 2017 af http://leikskolaborn.is/wp-content/uploads/2017/03/Cris-Rowan-Reykjavik-Conference-2017-Presentation.pdf.
16 Tick, B., Bolton, P., Happé, F., Rutter, M., & Rijsdijk, F. (2015). Heritability of autism spectrum disorders: a meta analysis of twin studies. Journal of Child Psychology and Psychiatry.
17 Phelan, J (2015, 24. Febrúar). Monsanto Glyphosate Roundup Herbicide Triggers Autism in Children. MIT Scientist. Global Reasearch. Sótt 15. maí 2017 af http://www.globalresearch.ca/monsanto-glyphosate-roundup-herbicide-triggers-autism-in-children-mit-scientist/5433023.
18 Beecham, J. E., & Seneff, S. (2016). Is there a link between autism and glyphosate-formulated herbicides? Journal of Autism, 3(1), 1.
19 Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Unwanted and wanted exposure to online pornography in a national sample of youth Internet users. Pediatrics, 119(2), 247-257.
20 Dunkley, V.L. (2014, 27. febrúar). Gray matters: Too much screen time damages the brain. Psychology Today. Sótt 15. maí 2017 af https://www.psychologytoday.com/blog/mental-wealth/201402/gray-matters-too-much-screen-time-damages-the-brain.
21 Dunkley, V.L. (2016, 31. desember). Autism and screen time: Special brains, special risks. Psychology Today. Sótt 12. maí 2017 af https://www.psychologytoday.com/blog/mental-wealth/201612/autism-and-screen-time-special-brains-special-risks.
22 Theoharides, T. C., Asadi, S., & Patel, A. B. (2013). Focal brain inflammation and autism. Journal of neuroinflammation, 10(1), 46.
23 Ranjbaran, Z., Keeffer, L., Stepanski, E., Farhadi, A., & Keshavarzian, A. (2007). The relevance of sleep abnormalities to chronic inflammatory conditions. Inflammation Research, 56(2), 51-57.
24 Björn Hjálmarsson (e.d.). Rafrænt skjáheilkenn – staðreynd eða mýta? Landspítalinn. Sótt 15. maí 2017 af http://www.landspitali.is/library/Sameiginlegar-skrar/Gagnasafn/Klinisk-svid-og-deildir/Kvenna--og-barnasvid/Gogn-fyrir-radstefnur/Hinn-gullni-medalvegur-Fyrir-lestrar-2017/bjorn-hjalmarsson.pdf.
25 Herbert, M. R., & Sage, C. (2013). Autism and EMF? Plausibility of a pathophysiological link–Part I. Pathophysiology, 20(3), 191-209.
26 O'Keeffe, G. S. (e.d). Teen Issues and Social Media: Which came first: the issues or the Apps? Landspítalinn. Sótt 15. maí 2017 af http://www.landspitali.is/default.aspx?pageid=00790bd9-4113-4429-b2f3-c0e6cd3e21d5

UT-VERÐLAUN SKÝ 2017
AÐGERÐARGRUNNUR SAREYE

Verðlaunahafi upplýsingatækniverðlauna Skýr 2017

Forseti Íslands hr. Guðni Th. Jóhannesson afhenti Guðbrandi Erni Arnarsyni, framkvæmdastjóra SAReye UT-verðlaun Skýr 2017 á UTmessunni þann 3. febrúar.

Hugbúnaður sem hannaður er af SAReye til að halda utan um verkefnastjórnun fékk UT-verðlaun Skýr árið 2017. Hugbúnaðurinn, sem kallast „Aðgerðagrunnur“, er þungamiðjan í öllum björgunaraðgerðum Slysavarnarfélagsins Landsbjargar (SL) og aðgerðastjórnum Almannavarna um allt land. Í honum eru skráðar upplýsingar um hópa, björgunarmenn, tæki sem notuð eru í aðgerðum, samskipti, verkefni sem verða til og þarfnast úrlausnar sem og fjölbreytt skráning hvers kyns gagna sem snerta björgunaraðgerðir með einhverjum hætti.

Aðgerðagrunnurinn hefur gjörbylt allri vinnslu upplýsinga í verkefnum SL og auðveldar að rýna í gögn og sjá tengingar sem áður var erfitt að koma auga á. Með myndrænni framsetningu verkefna á korti hefur yfirsýn stjórnenda aðgerða aukist verulega. Einnig hefur afkastageta aðgerðastjórnenda aukist þar sem afar vel hefur tekist að styðja við verkferla leitar og björgunar með hagnýtingu upplýsingatækninnar. Sérstaklega hefur tekist vel að útfæra hugbúnaðinn þannig að hann styðji við jafnt dagleg smáverkefni einstakra sveita sem og umfangsmiklar björgunaraðgerðir sem kallar á samhæfingu margra björgunarsveita og annarra viðbragðsaðila yfir langt tímabil. Óhætt er að fullyrða að aðgerðagrunnurinn hafi þegar sannað gildi sitt, enda er um að ræða byltingu í söfnun og meðhöndlun tölfræðiupplýsinga frá aðgerðum. Björgunarmenn með á stundum hafa takmarkaða tölvukunnáttu hafa byrjað að skrá tölfræðiupplýsingar sem hefur ekki þekkst áður í félaginu að því marki sem nú er.

Fyrirtækið SAReye var stofnað 2013 og er gott dæmi um íslenskt hugvit sem þróað er af sérfræðingum tengdum björgunarsveitum til að leysa á sem bestan hátt þarfir þeirra sem vinna við erfiðar aðstæður. SAReye vann Gulleggið 2013 og tók í framhaldinu þátt í Startup Reykjavík. Saga þess frá því að hugmynd kviknar, hvernig stuðningsnet sprotaumhverfis á Íslandi styður við góðar hugmyndir sem blómstra og eru teknar í notkun, er lýsandi dæmi þess að styðja þarf vel við nýsköpunarumhverfi á Íslandi.

Hugbúnaðurinn hefur sýnt sig og sannað síðustu misseri í stórum verkefnum eins og eldgosinu í Holuhrauni, björgun við strand Akrafells, leitum að týndum loftförum, aðgerðum í fárviðrum og nú síðast við eina stærstu leit á Íslandi í janúar. Réttar upplýsingar til allra aðila geta skipt sköpum við aðgerðir sem þessar og aðgengi björgunaraðila að kerfinu í gegnum alls kyns tækjabúnað mikilvægur.

Uppruni SAReye tengist leitar- og björgunarstarfi en fyrirtækinu hefur tekist að þróa vöru sína yfir í aðra óskylda geira. Áhersla félagsins er nú á aðila sem telja má til mikilvægra innviða samfélags. Aðgerðagrunnur SAReye heldur t.d. utanum öll frávik í raforkudreifikerfi Landsnets og samstarf Landsnets og Landsvirkjunar í stýringu á uppistöðulónum. Nýjasta útgáfa hugbúnaðarins miðast við að efla samvinnu milli fyrirtækja með hnitmiðaðri upplýsingamiðlun og samvinnu í neyðaratvikum.

Það má með sanni segja að kerfi sem þetta snerti líf margra enda tölvutæknin að verða samofin daglegu lífi okkar allra.

Í valnefnd voru Skúli Eggert Þórðarson, Ríkisskattstjóri, Hjálmar Gíslason, QLIK, Ari Kristinn Jónsson, Háskólinn í Reykjavík, Kristinn Árni Lár Hróbjartsson, SUT, Eggert Claessen, Frumtak, Helga Dögg Björgvinsdóttir, Skýr og Arnheiður Guðmundsdóttir, Skýr. Verðlaunagripurinn er glerlistaverk eftir Ingu Elínu.

Valnefndin hafði skv. reglum að leiðarljósi að verðlaunin væru veitt fyrir framúrskarandi framlag á sviði upplýsingatækni, skapað verðmæti og auðgað líf Íslendinga með hagnýtingu á upplýsingatækni. Áhersla er lögð á að framlagið hafi þegar sannað sig með afgerandi hætti.

Upplýsingar um fyrri verðlaunahafa og reglur um veitingu UT-verðlauna Skýr er að finna á www.sky.is

VINDHÖGG, VÍSINDI OG GERVIGREIND Á STERUM

Kristinn R. Þórisson, prófessor við Háskólann í Reykjavík

Eftir að gervigreind komst í tísku fyrir svona u.þ.b. fjórum árum, þegar fólk hleypur ekki lengur í burtu þegar ég segi þeim að ég stundi rannsóknir í gervigreind, hef ég oft þurft að svara spurningunni „Hvað er gervigreind?“ Ég svara því stundum með annarri spurningu: „Hvað er greind?“ Sem er auðvitað dálítið óréttlátt, því eftir rúmlega 120 ár af rannsóknum í sálfræði og 60 ár af gervigreindarrannsóknum hefur enn ekki tekist að finna hina einu sönnu skilgreiningu eða grundvallarútskýringu á fyrirbærinu.

Eins og svo margt annað sem ber fyrir augu í okkar nánasta sem og fjarlægasta umhverfi, hvort sem heldur er skammtafræði nú á tímum eða stjörnur og himintungl fyrr á öldum, er erfitt að smætta niður flókin náttúrufyrirbæri sem við skiljum ekki. Það hindrar þó marga ekki í að reyna að skella fram skilgreiningu þegar ég skora á þá. Oftast eru tilraunirnar míglekar þegar betur er að gáð, enda um margslungið fyrirbæri að ræða. Skemmtilegt er þó frá því að segja að oft eru það leikmenn, frekar en gervigreindarsérfræðingarnir, sem hitta naglann á höfuðið í slíkum tilraunum, eða a.m.k. aðeins nær honum. Því oftar en ekki tala leikmenn um að eitt lykileinkenni greindar sé hversu fjölbreytt verkefni hún geti tekið sér fyrir hendur, hversu nytsamleg hún sé til að framleiða nýjar hugmyndir, og hvernig hún geri okkur kleift að dýpka skilning okkar á öllu milli himins og jarðar. Með öðrum orðum, hve ósérhæfð og alhliða mannleg greind sé.

Upphaf gervigreindarsviðsins er oft rakið til ráðstefnu sem haldin var í Darthmouth-háskóla í Bandaríkjunum 1957, þar sem saman voru komnir margir þeirra sem áttu eftir að marka stefnu sviðsins á komandi áratugum. Í upphafi voru gervigreindarmenn vongóðir um framfarir og árangur rannsókna sinna og spáðu reglulega að innan áratugar myndi tölva sigra heimsmeistara í skák. Það tók 40 ár þangað til sú spá rættist þegar tölva þróuð af IBM vann Gary Kasparov, sem þá var talinn meðal bestu skákmanna heims.

Það var engin tilviljun að IBM valdi að einbeita sér að þróun véla sem spiluðu skák. Upphafsmenn gervigreindarsviðsins höfðu fært sannfærandi rök fyrir því að greind væri upplýsingavinnsla og höfðu sett fram þá tilgátu að hugsun væri í raun táknavinnsla (e. symbol manipulation). Eins og landið lá fyrir gervigreindarvísindamönnum þess tíma var skák eitt skýrasta dæmið um slíka vinnslu með tákn: Tegundir leikmanna, staða þeirra á taflborðinu, og áhrif og afleiðingar ákvarðanna spilaranna á gang leiksins, voru tilvalin til að færa inn í hugbúnaðarheim -- það eina sem vantaði þá var greindin: greindin til að vinna með þessi tákn á þann hátt að úr hlytist heimsmeistari.

Tilgátan sem lá þar að baki var ekki aðeins sú að greind væri nauðsynleg til að spila skák, heldur hafði hún metnaðarfyllra inntak: Að skák á heimsmælikvarða krefðist alhliða (e. general) greindar; að hver sú vera -- maður, dýr, vél -- sem spilaði skák á við heimsmeistara yrði að hafa alhliða greind.

Nokkrir upphafsmanna gervigreindar höfðu á áratugunum tveimur fyrir sigur Deep Blue smíðað vélar sem telja má einlægar tilraunir til að „kenna vélum að hugsa“ -- að færa hugsun á tölvutækt form. Og þótt engin alhliða greind hafi reyndar komið útúr því voru menn þó sammála að þetta væri skynsamlegasta kenningin sem fram hafði komið um mannlega greind, enda var (og er) mannleg greind talin besta dæmið um alhliða greind.

Tilgátan sem vísindamenn IBM voru að sannreyna þegar Deep Blue og Kasparov settust niður til að tefla var því ekki bara sú hvort þeir gætu smíðað vél sem ynni heimsmeistara, heldur sú hvort þeir yrðu hugsanlega þeir fyrstu til að smíða raunverulega vitveru; vitveru sem gæti skákað manninum ekki bara í tafli, heldur í öllu.

Líklega verður að telja þessa tilgátu meðal þeirra alröngustu vísindalegu tilgátna 20. aldar, því Deep Blue var ekki aðeins algjörlega laus við alhliða greind, heldur tókst IBM á næstu árum, þrátt fyrir mikinn tilkostnað, ekki að nýta kerfið í neitt annað. Vissir hlutar þess, t.d. vélbúnaðurinn, höfðu þó eflaust áhrif á örgjörvahönnun IBM á næstu árum og áratugum, en Deep Blue sem kerfi var ekki nýtanleg í nein önnur verk -- niðurstaðan var sú að hér væri á ferðinni sérhannað kerfi með enga aðra nýtingarmöguleika en það sem það var smíðað fyrir.

Nýlegar rannsóknir sýna að það er lítil sem engin fylgni milli skákgetu og greindar hjá ungum börnum -- a.m.k. eins og hún mælist með greindarvísitölumælingum sálfræðinnar. Hins vegar segir það okkur ekkert sérlega mikið þar sem engar djúpar kenningar um greind liggja að baki þeim mæliaðferðum.

Á síðustu tveimur áratugum hefur ekki mikið breyst í gervigreindarrannsóknum hvað þetta varðar. Vissulega hafa orðið framfarir, og einhver skref tekin í átt að alhliða gervigreind, en þau skref eru hænuskref í átt að Everest -- á meðan flestir sækjast eftir að betrumbæta þær gervigreindaraðferðir sem til eru með smávægilegum viðbótum eru fáir sem engir að rannsaka fyrir alvöru hvernig við skapa má „alvöru gervigreind“ í vél. Sumir telja að það sé hvort sem er ekki hægt, aðrir að sú aðferðafræði sem beitt sé í dag sé sú besta og því tilgangslaust að reyna aðrar nálganir. Á meðan þetta er staðreyndin eru litlar ástæður til að hafa áhyggjur af því að vélarnar verði brátt svo klárar að þær geri mannskepnuna að þræl sínum.

Hvenær getum við þá átt von á því skilningur okkar á greind dýpki verulega? Það er erfitt að segja, en eitt er víst: ótímabærar skilgreiningar ber að forðast; þær laða fram falska öryggistilfinningu, leiða til rangra áherslna og afvegleiða frekar en afhjúpa.

Við getum átt von stórtækum framförum þegar við skiljum betur hvernig manshugurinn framkvæmir margt af sínum undraverðu aðgerðum svo sem fjölþætt nám, þekkingaryfirfærslu, afleiðslu, aðleiðslu, fráleiðslu, og hvernig hann fer að því að framleiða af sjálfsdáðum ný undirmarkmið eftir þörfum. Þegar við skiljum hugann sem heild. Upphafsmenn gervigreindarsviðsins reyndu þetta, en slógu töluvert af vindhöggum. Hversu stór þau munu reynast -- hversu langt er upp á tindinn -- getum við ekki mælt fyrr en við komumst þangað; fyrr en við höfum smíðað eitthvað sem líkist meira alhliða greind mannvera.

Gervigreindarrannsóknir síðustu 60 ára benda til að aðferðafræðin sem verið er að beita sé ef til vill ekki sú rétta. Hvaða aðrar leiðir eru vænlegri til árangurs er erfitt að segja til um, en til þess eru rannsóknir. Á meðan meginþorri gervigreindarrannsókna hverfist um hönnun sérhæfðra kerfa, og litlir sem engir fjármunir eru lagðir í róttækari nálganir, verður ofurgreindar vitvélar einungis að finna á hvíta tjaldinu. Þangað til er gervigreind bara sjálfvirkni á sterum.

EYÐUR
VERÖLD SEM VERÐUR

Um daginn prófaði ég að opna fyrir eldvegginn sem er í beininum á heimilinu til þess að geta tengst heimilistölvunni utanfrá. Ég var ekki fyrr búinn en logg-skráin á heimilistölvunni fór að sýna runu tilrauna til að tengjast utan úr heimi með alls kyns notendanöfnum og lykilorðum.

Þetta var eins og að taka flugnanet af sér við Mývatn. Ef ég hafði efast um hvort eldveggurinn væri nauðsynlegur efaðist ég ekki lengur. Ég ákvað að hafa beininn opinn áfram því það er framtíðin að geta tengst heimilinu frá Internetinu ekki satt? Ég las mér til um hvernig hægt væri að gera fjaraðgang öruggari og nú er hann það vonandi. Ég er líka aðeins lífsreyndari.

INTERNETIÐ ER KLÓAKRÖR MEÐ BAKFLÆÐIVANDAMÁL

Flestir einstaklingar hafa lítið þurft að hugsa um tölvuöryggi. Hingað til hafa flest heimili verið tengd út á við án þess að leyfa tengingar inn vegna þess að á heimilinu eru neytendur sem fara út á stóra vefi eins og Mbl eða Netflix en enginn tengist á móti. Þeir sem reka netþjóna fyrirtækja hafa þurft að axla mestu ábyrgðina á öryggismálum fram að þessu.

Það er reyndar alveg merkilegt hvað flestir hafa siglt áhyggjulausir í gegnum tölvuheiminn án þess að lenda teljandi ógöngum. Flestir tapa gögnum af því þeir afrituðu ekki diskinn sinn. Tölvuglæpir eru ekki orðnir að vandamáli í þeirra lífi.

Margir eru með sama einfalda lykilorðið alls staðar og nota ekki tvíþætta sannvottun (e. two factor authentication) nema þegar þeir tengjast bankanum. Hún á að gefa aukið öryggi, því sá sem þú reynir að tengjast hefur þá samband við þig til að tryggja að þú sért þú. Nú er fólk farið að nota símann til að tengjast bankanum og það er einmitt sami síminn og bankinn hefur samband við!

Ef þú týnir símanum og hann er ólæstur þá ert þú kominn inn í heim sársauka eins og einhver sagði.

Aðgangsstýring er ekki það sem ég hef mestar áhyggjur af. Tæknilega kunnum við að tryggja örugg samskipti og auðkenningu.

Vandamálin eru og verða mannleg og félagsleg. Allt er að verða svo tengt og fólk verður fljótt samdauna og ógagnrýnið á tækni.

Ég sé að sumir eru að kaupa sér Google Home hátalara fyrir heimilið sem getur kveikt á tónlist eða slökkt ljósin en hann tekur líka upp allt sem sagt er á heimilinu og getur sent það út ef Google skiptir um einkunnarorð - sem í dag eru „Don't be evil".

ERUM VIÐ AÐ UPPLIFA 1984?

Í bókinni 1984 var skjár á öllum heimilum sem sýndi áróður frá stjórnvöldum en hann innihélt líka myndavél og hljóðnema til að hægt væri að fylgjast með þegnunum.

Það má segja að við séum farin að setja þennan 1984 búnað upp hjá okkur fyrir eigin kostnað.

Í bókinni 1984 var líka rætt um að endurskrifa söguna í sífellu til að undirstrika að stjórnvöld hefðu aldrei gert mistök eða haft rangt fyrir sér. Bækur og greinar voru endurskrifaðar og frumritið hvergi til. Þetta minnir óneitanlega á veraldarvefinn. Timarit.is eiga safn af gömlum blöðum en við erum ekki að passa upp á að geyma það sem stóð á vefsíðum af sömu natni.

Um daginn var bíllinn minn rafmagnslaus hvað eftir annað. Það kostaði tvo rafgeyma áður en ég komst að því hvað var að. Nágranninn hafði fengið sér þráðlausa veðurstöð út á svalir sem útvarpaði hitastiginu á sömu tíðni og bíllykillinn minn notaði. Bíllinn hélt að til stæði að opna sig nokkrum sinnum á mínútu og kveikti á aðaltölvunni til að athuga hvort réttur lykill væri á ferð. Bíllinn var óvart fórnarlamb „denial of service" árásar.

Það er ekkert víst að óvinurinn verði mennsk vera. Kannski verða það bara algrímar hjá stórum fyrirtækjum sem gera líf okkar verra. Ég hef heyrt að verslanir fari á hausinn af því að Google Maps sendir fyrrum viðskiptavini eftir nýrri leið og verslunin er því ekki lengur í leiðinni. Flugvélar setja gat á malbikið í flugbrautunum því GPS lendingartækni sér til þess að hver einasta vél setur dekkin niður á sama stað.

Ef ég ætlaði að gera einhverjum mein þá fæst margvísleg tækni til þess fyrir skiptimynt á Ali Express.

Það er hægt að kaupa millistykki fyrir lyklaborðssnúrur sem taka upp alla vélritun. Ég get komið fyrir myndavél hjá óvini mínum og fylgst með öllum hans ferðum.

Ég get keypt box með sim korti fyrir fimmtíu dollara sem getur opnað hurð ef ég hringi í það. Það má svo nota þetta sama box til að sprengja sprengju eða kveikja í gaskút. Búnaðinum má koma fyrir með löngum

fyrirvara, svo þarf bara að fylgjast með falinni myndavél og sprengja sprengjuna ef réttur aðili er til staðar.

Ef ég ætlaði að smygla eiturlyfjum myndi ég kaupa dróna sem færi frá báti fyrir utan landið og flygi inn á land á GPS púnkt sem hefur verið fyrirfram ákveðinn.

Það hefur aldrei verið eins spennandi að gerast glæpon -- ef ekki væri fyrir allar fjárans gæslumyndavélarnar!

Margir nota sífellt forrit eins og Twitter og Strava sem leyfa öllum að fylgjast með ferðum viðkomandi -- hvort hann er til dæmis alltaf úti að hlaupa á sama tíma. Væntanlega er þá hentugt að brjótast inn.

Um daginn stóð til að leggja niður pappírspeninga og klink til að hægt væri að fylgjast betur með svartamarkaðsbraski. Það þarf ekki að taka fram að þá er hægt að fylgjast með öllum viðskiptum, alls staðar og alltaf.

Hér á Íslandi höfum við ekki miklar áhyggjur af hnýsni nágrannans, við treystum honum yfirleitt, og erum vön því að allir séu að kjafta um alla. En hvað ef það breytist? Nasistar nýttu sér hvað þjóðskráin í Þýskalandi var skilmerkileg en hún skráði meðal annars hverrar trúar allir voru.

Skömmu áður en nasistar náðu völdum skrifaði Stefan Zweig í bókinni „Veröld sem var“ að flestir vinir hans hefðu verið sannfærðir um að með tilkomu ritsíma og talsíma væri heimurinn orðinn svo lítill að stríð væru nánast útilokuð.

Fólk telur sig vita hvað aðrir eru að hugsa því flestir eru komnir inn í hjúp af fólki sem hugsar eins og það sjálft, þökk sé Facebook algrímum sem parar fólk nánast saman eftir áhugamálum. Stjórnmálin lenda í skotgröfum fyrir vikið því það er svo átakalaust að sameinast skoðanabræðrum sínum um að hneykslast á einhverjum í staðinn fyrir að reyna að skilja hann.

Á sama tíma og við dáumst að Internetinu hættir fólk að bólusetja sig og heldur að þróunarkenningin sé eins og hver önnur trúarbrögð og ætti varla að kenna í skólum.

Breytingarnar eru svo örar að jafnvel menn eins og Eyður getur ekki giskað á næstu skref.

Ég myndi hafa miklar áhyggjur af þessu en ég er kominn á lokastig athyglisbrests vegna þess að það er svo mikið framboð af greinum og myndum á netinu. Í gamla daga voru teiknimyndir sýndar á aðfangadag til að foreldrarnir gætu undirbúið jólahátíðina en nú eru teiknimyndir handa öllum alla daga ársins allan sólahringinn.

Ef fréttirnar hræða mig get ég alltaf skipt yfir á Game of Thrones.

Góðar stundir.

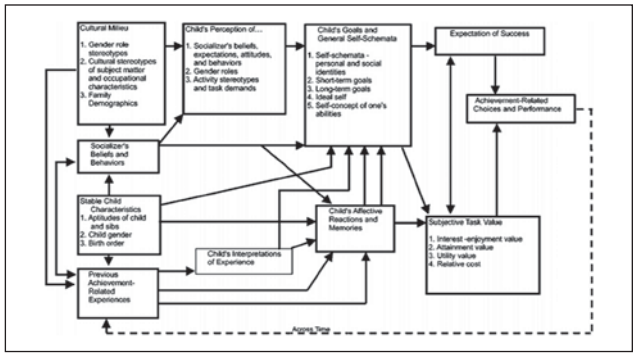
TÖKUMST Á VIÐ STAÐALÍMYNDIR

Dr. Ásrún Matthíasdóttir, lektor við Háskólann í Reykjavík

Hlutur kvenna í námi í tæknigreinum eins og tölvunarfræði hefur lítið breyst síðustu 20 ár þó ýmislegt hafi verið gert til að kynna námið fyrir þeim og auka áhuga þeirra. En hvers vegna eru stúlkurnar ekki í tækninámi? Þegar stórt er spurt er oft fátt um svör, en rýnum í málið og reynum að átta okkur á stöðunni. Athugum hvað rannsóknir segja okkur. Margar rannsóknir hafa verið gerðar á þessu sviðið og mynd 1 gefur nokkra hugmynd um viðfangsefnin þeirra.

Mynd 1. Dæmi um fyrirsagnir greina sem birta niðurstöður rannsókna um hvers vegna stúlkur sækja ekki í tæknigreinar

Ef við skoðum stöðuna hér á landi þá er hlutur kvenna í verkfræði, framleiðslu og mannvirkjagerð, raunvísindum, stærðfærði og tölvunarfræði frá 1997-2014 rúm 30% samkvæmt tölum frá Hagstofu Íslands. Ef þetta er skoðað nánar þá hafa kynjahlutföll í háskólanámi í raunvísindum, stærðfræði og tölvunarfræði frá 1997 til 2014 sveiflast á bilinu frá 35% í 40% og árið 2014 voru konur 36% nemenda í þessum greinum. Í verkfræði, framleiðslu og mannvirkjagerð hafa konur talsvert unnið á en þær voru 21% árið 1997, en voru komnar upp í 36% árið 2014. Á þessu tímabili hefur engin aukning orðið í tölvunarfræði, en hlutafallið var 22% árið 1997 og 21% árið 2014, mest var það 29% árið 2001 og fór niður í 13% árið 2010.



Mynd 2. Líkan Eccles og fleiri um væntanlegt áhrif á árangur (expectancy-value model of achievement, sjá Eccles, 1987, Eccles, Wigfield og Schiefele, 1998)

Margir þættir hafa haft áhrif á þróunina og mörg líkön hafa komið fram til að reyna að skýra áhrifavalda og til að skilja hvers vegna erfitt getur verið að breyta stöðunni. Til að sýna hversu flókið þetta er þá sýni ég hér módel Eccles og fleiri sem dæmi.

Ekki er svigrún til að skoða alla þættina sem koma fram á mynd 2, en rannsóknir hafa leitt í ljós að konur velja tölvunarfræðinám síður en karlar, meðal annars vegna skorts á sjálfstrausti, fyrirmyndum og hvatningu frá kennurum og foreldrum. Það sem ég ætla að skoða aðeins nánar eru fjórir áhrifaþættir: 1) Fjölmiðlar og dægurmenning, 2) áhrif jafningja og fjölskyldan, 3) samfélagshópar og fyrirmyndir og 4) áhrif menntunar – bæði formleg og óformleg áhrif.

Mynd 3. Myndir fengnar af netinu og sýna persónur í ýmsum myndum og sjónvarpsseríum

FJÖLMIÐLAR OG DÆGURMENNING

Forritarar starfa víða í dag, enda er forritun eitt af mörgum störfum sem fylgja hraðri þróun í upplýsingatækni. Það hafa myndast ákveðnar staðalímyndir í kringum forritara og aðra sem starfa við tölvur, sem eru jafnvel notaðar til að gera grín. Dæmigerðar eru persónurnar í „The Big Bang Theory". Við hlæjum öll að þeim. Þessar staðalímyndir þjóna sem hliðverðir (e. gatekeepers) og geta fælt stúlkur í burtu frá ákveðnum námsbrautum og því takmarkað námsmöguleika þeirra og starfsframa. Mynd 3 sýnir okkur nokkur dæmi úr vinsælum bíómyndum og sjónvarpsseríum.

Fyrirmyndir skapa ímyndir og hafa mikil áhrif og fyrir suma eru þessar fyrirmyndir aðlaðandi en fyrir aðra eru þær fráhrindandi. Mikilvægt er að stúlkur geri sér grein fyrir að þær þurfa ekki að vera ákveðin týpa til að læra ákveðna grein og þú þarft ekki að vera nörd til að læra tölvunarfræði. Til gamans læt ég einn nördabrandara fylgja: There are 10 types of people in the world: those who understand binary, and those who don't.

Mynd 4. Dæmi um aðstæður sem konur í tæknigreinum eru oft í.

ÁHRIF JAFNINGJA

Áhrif jafningja eru einnig mikilvæg og það getur verið erfitt að vera eina konan í hópnum. Vinnustaðamenningin skiptir miklu máli, það sem sést, heyrist, er gert og ímyndað, safnast saman í viðhorf sem síðan mótar líðan starfsmanna. Stúlkur eiga ekki bara erfitt með að samsama sig við karla á vinnustöðum, oft finnst þeim þær ekki heldur eiga samleið með öðrum stelpum á staðnum.

FJÖLSKYLDAN, SAMFÉLAGSHÓPAR OG FYRIRMYNDIR

Foreldrar hafa mikil áhrif á val á námi og starfi barna sinna. Stúlkur sem eiga mæður sem leggja áherslu á starfsframa hafa meiri metnað varðandi menntun og leita frekar í óhefðbundin kvennastörf. Rannsóknir hafa t.d. sýnt að menntun og viðhorf foreldra til tækni hefur áhrif þar sem foreldrar kaupa frekar vísindalega leiki eða leikföng handa strákum og trúa því frekar að þeir hafi áhuga á vísindum en foreldrar stúlkna. Foreldrar trúa að vísindi séu mikilvægari fyrir drengi og ætlast til meira af þeim á því sviði og ofmeta frekar getu drengja en stúlkna þegar kemur að námsgreinum tengdum vísindum. Mæður líta frekar en feður á vísindi sem óviðeigandi greinar fyrir stúlkur og koma þannig neikvæðu viðhorfi inn hjá þeim.

Talað er um að þessi viðhorf mótist snemma og þau séu jafnvel mótuð fyrir 14 ára aldur, en allt umhverfi barna hefur mótandi áhrif þó að mismikil séu og auðvitað geta viðhorf breyst alla ævi.

ÁHRIF MENNTUNAR – BÆÐI FORMLEG OG ÓFORMLEG

Lengi var í umræðunni að drengir væru einfaldlega betri en stúlkur í raungreinum, en það á sér ekki stoð í veruleikanum. Trú á eigin ágæti í stærðfræði, sem drengir hafa frekar en stúlkur, hefur verið talin geta haft áhrif á námsárangur og áhuga nemenda á tölvunarfræði. Í dag virðist þessi þáttur ekki lengur hafa eins mikil áhrif og áður, talið var að breytan skýrði 79% af muninum árið 1976 en ekki nema 13% árið 2011. Þetta er jákvæð þróun þar sem það hefur fylgt konum að meta eigin stærðfræðihæfni síðri en karla, jafnvel þær sem gengur vel/best telja sig ekki vera góðar í stærðfræði.

Námsumhverfið skiptir líka miklu máli. Hvatning og upplifun er mikilvæg og einfaldlega með því að breyta nafni á námsbrautum hefur tekist að auka aðsókn stúlkna í raungreinar. Það virðist ekki skipta öllu hvað er kennt heldur hvernig efnið er kennt. Kynin þykja leggja mismunandi áherslur á tæknileg atriði þar sem drengir beina meira athyglinni að stærðfærði og vélbúnað en stúlkur hafa oft meiri áhuga á sköpun, samskiptum og atvinnumöguleikum sem tengjast tækninni. Þetta gefur menntakerfinu tækifæri til að leggja meiri áherslu á fög og skipulag sem getur hentað stelpum betur og með því að bjóða upp á öðruvísi og fjölbreyttari verkefni í meira skapandi umhverfi er hugsanlega hægt að auka áhuga þeirra á tæknigreinum.

Árið 2016 gerði höfundur könnun meðal nemenda í tölvunarfræði við Háskólann í Reykjavík sem 138 konur tóku þátt í. Þar kom fram að konur eru hagsýnar í hugsun þegar kemur að vali á námi og völdu tölvunarfræði því þær töldu sig geta fengið vel launuð störf og góða atvinnumöguleika, jafnvel þótt þær hefðu frekar viljað læra eitthvað annað. Tæpur helmingur þátttakenda sagðist seint hafa fengið áhuga á tölvum, eða eftir 22 ára aldur, og fóru því frekar seint í tölvunarfræðinám og jafnvel eftir að hafa lokið öðrum gráðum í óskyldum fögum, s.s. lögfræði og hjúkrun. Þær voru ánægðar í náminu og hlökkuðu til að vinna á sviðinu. Þær töldu sig ekki hafa góða tölvufærni þegar þær byrjuðu í náminu, en um helmingur þeirra hafði notað tölvur sem unglingar og þá aðallega í grunnskólum og framhaldsskólum í tengslum við nám.

Sérhvert þjóðfélag þarf á þátttöku beggja kynja að halda í uppbyggingu á tækni- og upplýsingageiranum sem og í öðrum greinum. Margt hefur verið gert hér á landi til að auka áhuga stúlkna á tæknigreinum og byggja upp tenglanet þeirra á milli, s.s unnin kynningarmyndbönd, bæklinga gefnir út, vefsíður settar upp, grasrótarsamtök stofnuð og skóla og fyrirtæki heimsótt. Ég nefni sem dæmi störf UT-kvenna, samtökin /sys/tur, Stelpur og tækni daginn í HR og WomenITechIIceland.

Það er greinilegt af gröfunum hér fremst að viðhorfsbreytingar taka tíma en við getum ekki gefist upp því við þurfum að kynna fyrir báðum kynjum sem flesta möguleika á námi og starfi svo þau geti tekið upplýsta ákvörðun. Við þurfum að takast á við staðalímyndir!

HEIMILDIR KOMA VÍÐA AÐ OG NEFNI ÉG ÖRFÁAR HÉR:

Ásrún Matthíasdóttir og Jóna Pálsdóttir. (2017). Where are the girls in STEM? Ráðstefnurit: 6th STS Italia Conference Sociotechnical Environments, Trento, Ítalía.

Ásrún Matthíasdóttir og Kristine H. Falgren (2015). Hvað þarf til að auka áhuga kvenna á tölvunarfræði? Tölvumál á vefnum.

Ásrún Matthíasdóttir og Kristine H. Falgren (2013). Konur og tölvunarfræði. Tölvumál, 38, 1.

Cheryan, S., Master, A. og Meltzoff, A. N. (2015). Cultural stereotypes as gatekeepers: increasing girls' interest in computer science and engineering by diversifying stereotypes. Front Psychol, 6: 49.

Gürer, D. og Camp, T. (2002) Investigating the Incredible Shrinking Pipeline for Women in Computer Science. Final report.

Linda J. Sax, Kathleen J. Lehman, Jerry A. Jacobs, M. Allison Kanny, Gloria Lim, Laura Monje-Paulson & Hilary B. Zimmerman. (2016). Anatomy of an Enduring Gender Gap: The Evolution of Women's Participation in Computer Science. The Journal of Higher Education, online.

Lang, C., Fisher, J. Craig, A. og Forgasz, H. (2015). Outreach programmes to attract girls into computing: how the best laid plans can sometimes fail. Computer Science Education. 25, 3.

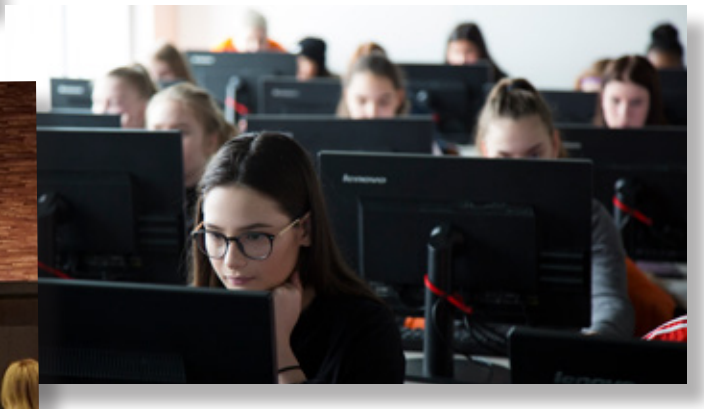
Phukan, D. og Dr. Saikia, J. (2017). Parental Influence, Gender Socialization and Career Aspirations of Girl Students: A Study in the Girls' Colleges of Upper Assam. International Journal of Research in Humanities and Social Studies. 4, 2, pp. 31 -37.

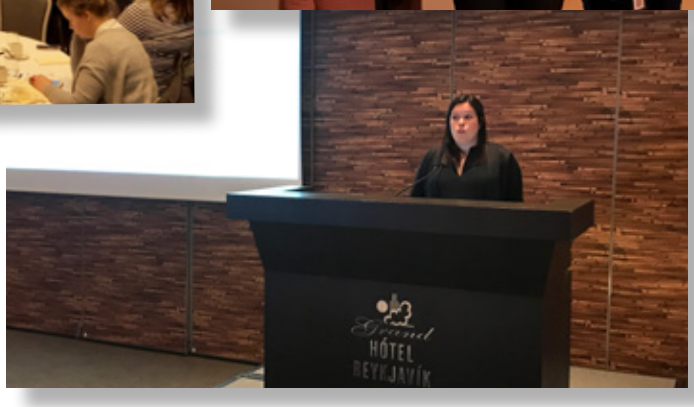
Myndir eru síðan fengnar héðan og þaðan á netinu.

SÍÐAN SÍÐAST...

Það sem af er árinu 2017 hafa verið haldnir um 15 viðburðir. Til viðbótar eru á teikniborðinu allmargir viðburðir fram að jólum og framundan fróðlegur vetur hjá félaginu. Flaggskipið er UTmessan sem verður haldin í áttunda sinn í Hörpu 2. og 3. febrúar 2018 en undirbúningur fyrir hana er í gangi allt árið og áhugi erlendra aðila á UTmessunni er sífellt að aukast.

Vel hefur gengið að skipuleggja dagskrá viðburða sem er að mestu í höndum faghópa innan Ský. Hægt er að nálgast dagskrá og upplýsingar um viðburðina ásamt glærukynningum á vefnum sky.is.





YFIRLIT YFIR LIÐNA VIÐBURÐI FRÁ ÞVÍ SÍÐUSTU TÖLVUMÁL KOMU ÚT:

Október	Hvert stefnum við í innleiðingu á snjallausnum
Nóvember	Hugbúnaðargerð í skýinu
Nóvember	Rekstur netkerfa
Desember	UT-dagurinn
Desember	Prófanir vefja
Janúar	Hvert stefnir rafræn opinber þjónusta
Febrúar	UTmessan – ráðstefna og sýning
Febrúar	Heilbrigðisráðstefnan
Febrúar	Aðalfundur Öldungadeildar
Febrúar	Aðalfundur Ský
Mars	Öryggi hins opinbera
Mars	Vefir og appþróun
Apríl	Nýjungar í fjarskiptum
Maí	Samfélagsmiðlar
Maí	Rekstur í skýjunum
Ágúst	Fagmennska í íslenskum vefbransa
September	Stefnumótun faghópa og stjórnar Ský
September	Heitustu málin framundan í tölvugeiranum

Drög að dagskrá vetrarins 2017-2018 má finna á sky.is

FRÉTTIR AF STARFSEMI SKÝ

Arnheiður Guðmundsdóttir, framkvæmdastjóri Skýs


Vetrarstarfið er nú komið af stað af fullum krafti og sjá Arnheiður Guðmundsdóttir og Hildur Rut Halblaub um alla þræði starfseminnar. Mörg járn eru í eldinum að venju og því nóg af verkefnum framundan hjá Ský.

Þar sem félagið verður 50 ára í apríl 2018 ákvað stjórn Skýs að fara í stefnumótunarvinnu og skerpa á starfseminni til framtíðar og verður niðurstaða þeirrar vinnu kynnt síðar í vetur. Stefnt er að því að halda upp á afmælið og fagna í leiðinni útkomu bókar um tölvuvæðingu á Íslandi 1964-2014 en söguna er nú þegar hægt að skoða á vefsvæðinu sky.is og óskum við enn og aftur eftir myndum til að skreyta bókina. Myndirnar þurfa að vera í góðri upplausn og leyfi höfundar að fylgja með. Ákveðið var að taka saman söguna þar sem 50 ár voru liðin frá því að fyrsta alvöru tölvan kom til landsins. Reynt er að stikla á stóru um það sem gerðist á þessum árum og er sögunni skipt í fimm 10 ára tímabil. Ekki er ætlunin að telja upp öll verkefni, fyrirtæki eða aðila sem komu að verkinu en hins vegar erum við að safna saman lista yfir þau fyrirtæki sem tengjast tölvugeiranum á þessum árum ásamt 2-3 setningum um fyrirtækið og setjum á vefinn. Allar fyrirspurnir, myndir og annað má senda á sky@sky.is.

Ýmis önnur verkefni eru í gangi hjá félaginu fyrir utan að halda viðburði. Tímaritið Tölvumál hefur verið gefið út frá árinu 1976, árlega á prenti en vikulega er birt ný grein í Vefútgáfu Tölvumála á forsíðu www.sky.is. Þar geta allir sent inn greinar og pistla en þeir mega vera um hvaða efni sem er tengdu tölvu- eða tæknimálum. Árlega veitir félagið Upplýsingatækniverðlaun Skýs og á aðalfundum félagsins eru heiðursfélagar tilnefndir þegar tilefni er til.

Helstu verkefni innanlands eru að halda fróðlega viðburði fyrir félagsmenn og aðra í tengslaneti Skýs og eru 2-3 fræðsluviðburðir í hverjum mánuði yfir vetrartímann. Stærsti viðburðurinn er eins og áður UTmessan sem félagið setti af stað 2011 þar sem vöntun var á stórum óháðum tölvu- og tækniviðburði sem felur í sér metnaðarfulla ráðstefnu og sýningu á helstu tækni og nýjungum sem fyrirtæki landsins tengdum tölvugeiranum vinna við. Megintilgangur UTmessunnar er að vekja athygli á hve mikil gróska er í tölvu- og tæknigeiranum með það markmið að hvetja ungt fólk til að velja sér tæknigreinar sem framtíðarstarf. UTmessan hefur vakið athygli erlendis þar sem öll Evrópulönd glíma við sama vanda en mikil vöntun er á tölvufólki um allan heim í nánustu framtíð.

Óhætt er að segja að UTmessunni hafi verið tekið vel frá upphafi og nú er svo komið að erlendir fyrirlesar sýna frumkvæði að því að senda inn tillögur að fyrirlestrum, erlendir gestir farnir að mæta til landsins á UTmessuna og síðast en ekki síst eru erlend fyrirtæki farin að sækjast eftir að vera á sýningarsvæðinu. Það er kærkomin viðbót við gífurlega góðann og jákvæðan stuðning allra þeirra flottu íslensku fyrirtækja og skóla sem taka þátt í UTmessunni og erum við löngu komin að þeim tímamótum að Harpa okkar glæsilega ráðstefnuhús hefur ekki nóg pláss til að taka á móti öllum þeim sem vilja vera á sýningarsvæði UTmessunnar en erfitt er að finna aðra aðstöðu þar sem ráðstefnusalir og sýningarsvæði eru á sama stað. Við leitumst við að reyna að koma öllum fyrir en því miður hefur selst upp bæði á ráðstefnuna og sýningarsvæðið löngu fyrir UTmessu.

Ský er aðili að evrópsku samtökunum CEPIS en það er félag með öllum tölvufélögum í Evrópu. Þar starfa nokkrir faghópar og höfum við verið virk innan Women in ICT, Education in ICT og Ethics in ICT. Þar höfum við lagt fram tillögur og verkefni sem Evrópusambandið hefur oftar en ekki tekið áfram í sitt starf en öll þessi málefni eru heit í fleiri löndum en hér á Íslandi. Forritun sem skyldufag í grunnskólum er t.d. eitt af því sem öll löndin eru að berjast fyrir og því ekki sérílenskt að pressa á menntayfirvöld með það.

Eitt af þeim verkefnum sem við tengjumst í gegnum CEPIS er að halda í apríl ár hvert „Girls in ICT Day“ og höfum við verið þátttakendur í því á Íslandi með Háskólanum í Reykjavík og fleiri aðilum síðustu ár. Þar er einn eftirmiðdagur tekinn í að bjóða stelpum í ákveðnum árgangi að mæta á stutt námskeið tengd tölvunarfræðum og svo fara þær í heimsókn og leysa skemmtileg verkefni hjá tölvufyrirtækjum í Reykjavík. Dagurinn í ár tókst vel og vonandi tókst að koma tölvugeiranum á blað hjá stelpunum þegar að því kemur að þær velji sér framtíðarmenntun og starfsvettvang.

Síðustu 2 ár höfum við tekið þátt í alþjóðlegu verkefni sem heitir BEBRAS „International Challenge on Informatics and Computational Thinking“ (bebras þýðir bifur, enska heitið beaver) en það miðar að því að árlega keyra öll lönd í heiminum í eina viku verkefni þar sem krakkar á aldrinum 6-18 ára leysa þrautir á vef sem eru uppbyggðar eins og forritun, þ.e. þrautir sem fá krakka til að hugsa eins og þau væru að forrita en þrautirnar eru ekki forritun sem slík. Síðasta ár tóku 18 skólar á Íslandi þátt, 1875 nemendur og gaman að segja frá því að verkefnið tókst vel og stelpurnar sem tóku þátt fleiri en strákarnir enda tölvugeirinn einn af þeim geirum sem hentar báðum kynjum. Vikuna 6. – 10. nóvember verður BEBRAS keyrt og geta allir skólar sem vilja skráð sig í gegnum www.bebras.is.

Félagið vinnur náið með ráðuneytum og fyrirtækjum landsins og er Ský með fulltrúa í stjórn Persónuverndar skv. lögum en auk þess eru félagsmenn oft kallaðir til verkefna svo sem vinnuhóp um landsumgjörð og fleira í þeim dúr. Það er mikilvægt að halda fagmennsku félagsins áfram enda er Ský óháð „non-profit“ félag stofnað árið 1968 og hefur síðan þá verið í forsvari og fararbroddi sem málsvari allra þeirra sem vinna að eða hafa áhuga á tölvumálum. Langar mig að þakka sérstaklega þeim sem taka þátt fyrir hönd félagsins í verkefnunum því oftar en ekki er um ólaunað starf að ræða.

Að lokum er vert að nefna að stjórnir faghópa, orðanefnd og ritnefnd vinna ötull starf sem heldur félaginu gangandi og mikill hugur í fólki. Allt starf Skýs er unnið undir dyggri stjórn félagsins en þar er úrvalslið sem er mjög vel tengt í tölvugeirann og stútfullt af skemmtilegum hugmyndum um félagsstarfið.

Hér sjáið þið mynd af þeim sem skipa stjórnina.

Stjórn Skýs 2017-2018

Ég hvet ykkur til að vera í sambandi ef eitthvað er og einnig að tengjast Skýs á Facebook, LinkedIn og Twitter í gegnum forsíðu sky.is og taka þátt í umræðum þar. Sjáumst á viðburðum í vetur.

Náðu forskoti með lausnum frá Advania

Einstaklingar og allar stærðir fyrirtækja geta sótt til okkar stakar lausnir eða samþætta heildarþjónustu því lausnaúrval okkar spannar upplýsingatækni í sinni breiðustu mynd

Hafðu samband og við hjálpum þér að ná forskoti með snjallri notkun upplýsingatæknilausna.

440 9000
advania.is | advania@advania.is

advania
Welcome to IT

Við höfum góða reynslu af framtíðinni

NÝHERJI / BORGARTÚNI 37, MÁN.-FÖS. KL. 9-18 & LAU. KL. 11-15 / KAUPANGI AKUREYRI, MÁN.-FÖS. KL. 9-17 / **NETVERSLUN.IS**