ÞJÓNUSTA FYRIR ÞIG

REYKJAVÍKURBORG

Áhrif notkunar samfélagsmiðla á netöryggi Reykjavíkurborgar

Jón Ingi Þorvaldsson, deildarstjóri Upplýsingatæknideildar

Kveikjan að verkefninu

- Frétt á mbl.is 28.jan. 2015 með fyrirsögninni „Facebook má skoða allt“.

Innlent | mbl | 28.1.2015 | 18:10

Facebook má skoða allt

Facebook hefur nú víðtæka heimild til að sækja upplýsingar úr tækjum og tölvum notenda sinna. AFP

Allir þeir sem hafa farið inn á Facebook eftir 1. janúar hafa veitt fyrirtækinu leyfi til að safna upplýsingum af öllum tækjum sem notuð eru til að fara inn á samskiptamiðilinn. Ekkert verndar fólk fyrir því að löggæsluaðilar fái aðgang að þeim gögnum, að sögn ráðgjafa hjá Deloitte.

Nýir notendaskilmálar tóku gildi á Facebook 1. janúar og fjallaði Ævar Einarsson, liðsstjóri upplýsingatækniráðgjafar Deloitte, um þá á málþingi Persónuverndar um rafrænt eftirlit í dag. Þeir veita bandarísku fyrirtækinu víðtækar heimildir til þess að safna upplýsingum um notandann sem hann hefur enga stjórn yfir, án þess hreinlega að hætta að nota miðilinn.

Ævar benti á að áætlað væri að 70% af öllum nettengdum fullorðnum einstaklingum í heiminum séu með Facebook-aðgang. Fyrirtækið sitji þannig á miklum upplýsingum um heiminn. Þær upplýsingar skiptist í tvo flokka, annars vegar þær sem fólk setji sjálfviljugt inn, myndir, stöðuuppfærslur og ummæli, og hins vegar fullt af upplýsingum sem skapast við notkunina. Þar á meðal eru upplýsingar um staðsetningu notandans og IP-tölu.

Kemst í sms, símtöl, pósta og leitarsögu

Ákvæði nýju notendaskilmálanna gera Facebook nú kleift að safna alls kyns upplýsingum af símum, spjaldtölvum og jafnvel vinnutölvum fólks. Ekki þurfti að samþykkja skilmálana sérstaklega heldur töldust þeir samþykktir um leið og fólk fór inn á Facebook eftir 1. janúar. Ævar sagði að á meðal þessara

Kveikjan að verkefninu

- Frétt á mbl.is 28.jan. 2015 með fyrirsögninni „Facebook má skoða allt“.
- Í kjölfarið kom beiðni frá innri endurskoðun um að greina hugsanleg áhrif á net- og upplýsingaöryggi.
- Leitað eftir sérfræðiráðgjöf frá Capacent.
- Ákveðið að útvíkka verkefnið þ.a. það næði yfir notkun helstu samfélagsmiðla
- Einnig skoðuð áhrif notkun snjalltækja almennt.

Markmið og ávinningur verkefnis

- Að fá yfirsýn yfir notkun samfélagsmiðla hjá starfsmönnum Reykjavíkurborgar.
- Að leggja mat á áhrif notkunar samfélagsmiðla á net- og upplýsingaöryggi hjá Reykjavíkurborg.
- Að draga fram upplýsingar um það hvaða eftirlitsaðgerðir eru til staðar og hvaða ráðstafanir þurfi að gera.
- Að stjórnendur öðlist yfirsýn varðandi áhættu tengdri notkun samfélagsmiðla og áhrif á net- og upplýsingaöryggi.
- Að greining geti nýst við mótun stefnu og leiðbeinandi tilmæla um ábyrga notkun samfélagsmiðla fyrir starfsmenn borgarinnar.

Hverju safna samfélagsmiðlar?

facebook LinkedIn Google

- IP tala
- Vafri (IE, Chrome o.s.frv.)
- Stýrikerfi (Windows, Mac o.s.frv.)
- Heimsóttar vefsíður (browsing history)
    - (Like takki, Share to Twitter, LinkedIn, Google+)
- Staðsetning (GPS)

facebook Google

- Upplýsingar um tækið (hugbúnað, vélbúnað, rafhlaða, o.fl.)
- WiFi – Hvaða þráðlausu netum sem tækið hefur tengst
- Farsímanúmer (eingöngu farsímar)

facebook LinkedIn

- ISP (*Internet Service Provider* - Internetveita)
- Upplýsingar sem veittar eru vegna samtengingar við tengiliðaskrá (Finna fleiri vini/tengiliði með því að deila tengiliðaskrá, að gefnu samþykki)

Google

- Öll leitarorð notanda að því gefnu að viðkomandi notandi sé skráður inn í vafrann með Gmail aðgangi sínum. Þó er ekki hægt að fullyrða að notandi þurfi að vera skráður inn í vafrann með Gmail aðgangi sínum.

Helstu niðurstöður

- Ekki er vitað til þess að upp hafi komið öryggis-atvik tengd notkun starfsmanna á samfélagsmiðlum.
- Metnar voru 11 tilteknar hættur og voru 3 þeirra taldar óásættanlegar en aðrar voru innan áhættuviðmiða.
- Helstu hættur sem metnar voru tengdust notkun snjalltækja og miðlun viðkvæmra upplýsinga almennt en ekki samfélagsmiðlunum sjálfum.

Helstu hættur sem metnar voru

- Vistun viðkvæmra upplýsinga á fartækjum (fartölvum/ farsímum/ spjaldtölvum), s.s. persónu- eða fjárhagsupplýsinga. Geta komist í rangar hendur ef tæki týnist eða er sent í viðgerð.
- Starfsmenn geta sett hvaða öpp sem er upp á snjalltæki. Þar á meðal kunna að vera öpp sem innihalda njósnabúnað.
- Hætta er á að starfsmenn tjái sig á samfélagsmiðlum um viðkvæmar persónugreinanlegar upplýsingar um umbjóðendur borgarinnar.

Aðrar hættur tengdar samfélagsmiðlum

- Óæskileg myndbirting á samfélagsmiðlum af börnum eða ungmennum.
- Hætta á að óviðkomandi aðilar hafi aðgang að hópum á samfélagsmiðlum sem stofnaðir hafi verið utan um deildir eða innri verkefni borgarinnar.
- Hætta á að starfsmenn noti sömu lykilorð að samfélagsmiðlum og innri kerfum borgarinnar.
- Hætta á smiti af „tölvuóværu“ frá samfélagsmiðlum.

Leiðir til úrbóta

- Auka öryggisvitund starfsmanna.
- Dulkóða gögn á fartækjum (farsímum/ spjaldtölvum/ fartölvum) sem tengjast innri kerfum borgarinnar, s.s. tölvupósti og fjárhagsbókhaldi.
- Athuga þörf á stýringu snjalltækja sem tengjast innra neti og innri kerfum.
- Endurskoða aðgengismál snjalltækja að þráðlausu neti.
- Móta stefnu um ábyrga notkun samfélagsmiðla.
- Móta stefnu um notkun eigin tækja (BYOD).

Spurningar?

Viðauki - Áhættulisti

ÁHÆTTUFLOKKUR	LÝSING ÁHÆTTU	MEÐHÖNDLUN ÁHÆTTU
Rekstraráhætta	Hætta er að óviðkomandi aðili komist yfir aðgangs- eða viðkvæmar upplýsingar. Þetta er vegna þess að UTD hefur ekki stjórn á hvaða forrit (app) eru sett upp á tæki. Hætta er á að í einhverjum forritum sé njósnabúnaður eða önnur forrit sem gætu afritað þessi gögn eitthvert annað. Notkun snjalltækja er mikil hjá stjórnendum og kjörnum fulltrúum sem hafa þannig aðgang að viðkvæmum upplýsingum. Vitund starfsmanna á þessari tegund áhætta er takmörkuð.	Lagt er til að skoðað sé hvort ástæða sé til að skoða lausnir sem gera kleift að stýra snjalltækjum og þá hvaða smáforrit má setja upp og þá hvernig stjórnun á aðgangi að póstkerfi sé stillt. Þetta er t.a.m. hægt með mobile device management lausn.
Orðsporsáhætta	Áhætta er að óæskileg myndbirting, t.d af börnum eða ungmennum, sé miðlað á samfélagsmiðlum og rati í rangar hendur. Slík myndbirting gæti valdið viðkomandi einstakling skaða en einnig að slíkum myndum væri miðlað á óæskilegan máta. Vitað er til dæma þar sem atvik af þessum toga hafa komið upp með notkun forritsins Snapchat. Í vinnslu er mótun á viðmiðum SFS sviðs	
Hlítingaráhætta	Hætta er að á síma geti verið viðkvæmar fjárhagsupplýsingar sem geta orðið aðgengilegar óviðkomandi aðilum þegar tæki fer í viðgerð. Það eru ca 600 tæki sem eru tengd með Active sync og tölvupóst í tæki. Þegar tæki fara í viðgerð er líklegt að á þessum tækjum séu viðkvæm gögn og á meðan þau eru í viðgerð eru líkur á að óviðkomandi komist yfir þessi gögn.	Lagt er til að skoðað verði hvort hægt væri t.d. að semja við þjónustuaðila um að sjá um viðgerð tækja og að þar séu sérstakir skilmálar um öryggi. Jafnvel væri hægt að kanna hvort það teljist ásættanleg áhættumeðhöndlun að innleiða mobile device management laus. Þar væri hægt að stýra betur stillingum í snjalltækjum.
Hlítingaráhætta	Hætta er að á síma geti verið viðkvæmar persónuupplýsingar sem geta orðið aðgengilegar óviðkomandi aðilum þegar tæki fer í viðgerð. Það eru ca 600 tæki sem eru tengd með Active sync og tölvupóst í tæki. Þegar tæki fara í viðgerð er líklegt að á þessum tækjum séu viðkvæm gögn og á meðan þau eru í viðgerð eru líkur á að óviðkomandi komist yfir þessi gögn.	Lagt er til að skoðað verði hvort hægt sé að setja vinnureglur um að öll tæki fari á tiltekinn stað til viðgerða. Einnig er mikilvægt að skoða högun vegna eignahalds á snjalltækjum. Einnig lagt til að settar séu reglur um þegar starfsmenn fara með tæki í viðgerð.
Hlítingaráhætta	Hætta er brot á Persónuverndarlögum vegna þess að óviðkomandi aðili (t.d. Facebook) gæti haft aðgang að gögnum í tölvum starfsmanna og birt þær opinberlega. Innan borgarinnar, og í einstaka tilvikum til annarra stofnana, löggæsluaðila, er verið að senda mjög viðkvæmar persónuupplýsingar í tölvupósti, bæði í innihaldi pósts og í viðhengi. Ekki eru til staðar reglur um hvernig samskipti við ytri aðila skulu fara fram né hvernig umgangast skal gögn á sameiginlegum netsvæðum. Tölvur eru tengdar á samtengd netdrif þar sem unnið er með viðkvæmar upplýsingar. Í einhverjum tilfellum er heimilt er að tengjast með VPN tengingu inn á innra net borgarinn frá heimatölvu. Þó er ekki vitað til þess að tilfelli hafi komið upp þar sem notkun samfélagsmiðla ógnaði net- og upplýsingaöryggi borgarinnar.	Lagt er til að skoðað verði hvort hægt sé að setja stefnu um notkun samfélagsmiðla og að skerpa á verklagi og jafnvel setja reglur um miðlum viðkvæmra upplýsinga til ytri aðila.
Hlítingaráhætta	Áhætta er að starfsmaður tjái sig á samfélagsmiðli sem getur valdið því að viðkvæmar persónugreinanlegar upplýsingar um umbjóðenda borgarinnar rati í rangar hendur. Notkun samfélagsmiðilsins Facebook er að aukast. Tilfelli sem þessi geta talist trúnaðarbrot í starfi.	
Rekstraráhætta	Áhætta er að óviðkomandi aðili sé meðlimur í hóp sem stofnaður hefur verið á Facebook og notaður er af starfsmönnum, og hafi þannig mögulegan aðgang að viðkvæmum upplýsingum, t.d. um meðlimi þeirra hópa, símanúmer eða um verkefni þeirra. .	
Orðsporsáhætta	Hætta er að óviðkomandi aðili, hvort sem það er Facebook eða annar, geti haft aðgang að upplýsingum sem deilt er á Facebook í gegnum hópa sem gerðir eru og birt þær opinberlega. Vitað er til þess að starfs- eða stýrihópar noti samfélagsmiðilinn Facebook til að mynda hópa tengda ákveðnum verkefnum sem verið er að vinna hverju sinni. Ólíklegt er að starfsmenn eða kjörnir fulltrúar seti inn mjög viðkvæmar upplýsingar inn á slíka hópa. Ekki eru þekkt dæmi um að slíkar upplýsingar hafi verið gerðar opinberar. Vitað er til að settar séu reglur um notkun í haus á tilteknum hópum Facebook þar sem fram koma almennar leiðbeiningar um notkun og að gagnasvæði séu sérstaklega opnuð til að veita aðgang að viðkvæmum upplýsingum.	
Rekstraráhætta	Hætta er að starfsmenn noti samskonar lykilorð til að auðkenna sig inn á Facebook og að kerfum borgarinnar, þannig að ef óviðkomandi aðili kemst yfir eitt lykilorð, til dæmis að Facebook, gæti þá viðkomandi reynt að geta sér til um notendakenni starfsmanns og þannig komist yfir aðgang að tölvupósti. Ekki eru til staðar þekkt dæmi um að þessi hætta hafi raungerst.	
Rekstraráhætta	Hætta er að tölvuóværa smiti tölvu og þessi óværa geti mögulega læst öllum gögnum eða sett inn njósnabúnað sem getur leitt til rekstrartruflunar. Notkun á samfélagsmiðlum getur opnað á að óværa komist inn í tölvu. Í stillingum hjá Facebook er mögulegt að svindl- og smitpóstar komist í framhjá ruslsíum þar sem póstur sendur á Facebook póstfang er mögulega sendur áfram á vinnupóstfang.	
Hlítingaráhætta	Hætta er brot á Persónuverndarlögum vegna þess að óviðkomandi aðili (t.d. Facebook) gæti haft aðgang að upplýsingum sem eru í tölvupósti starfsmanna. Heimilt er að tengjast tölvupósti frá símtæki eða spjaldtölvu hafi verið fengin til þess heimild, og vitað er til að notkun er jafnt á eigin tæki og tækjum á vegum borgarinnar. Innan borgarinnar, og í einstaka tilvikum til annarra stofnana, löggæsluaðila, er verið að senda mjög viðkvæmar persónuupplýsingar í tölvupósti, bæði í innihaldi pósts og í viðhengi. Ekki eru til staðar reglur um hvernig samskipti við ytri aðila skulu fara fram. Þó eru ekki dæmi um að tilvik eins og þessi hafi komið upp.	