NETÖRYGGI HJÁ REYKJAVÍKURBORG

Innri endurskoðun

05.04.2018

Meginþættir

- Umfang og aðferðafræði
- Helstu áhættuþættir
- Helstu ábendingar
- Viðbrögð stjórnenda

Markmið úttektarinnar var að fá mynd af þeim öryggisráðstöfunum sem til staðar eru hjá Reykjavíkurborg og varða almennt netöryggi.

Ekki er hægt að benda á neitt eitt atriði sem hefur úrslitaáhrif á netöryggi. Margir þættir spila þar saman en mannlegi þátturinn vegur þó alltaf þyngst. Almenn vitund og þekking starfsfólks á upplýsingaöryggi er eitt veigamesta atriði netöryggis hjá fyrirtækjum, enda skiptir engu máli hve mikið er lagt í tæknilegar lausnir ef starfsfólk er ekki meðvitað um þá öryggisþætti sem skipta máli.

Fyrirtæki þurfa að meta hversu langt þau eiga að ganga í að setja upp tæknilegar lausnir til að verja ákveðin gögn eða kerfi, en hafa þarf í huga leynd, réttleika og tiltækileika þeirra gagna og kerfa sem um ræðir þegar mat er lagt á ásættanlegt öryggi.

UMFANG OG AÐFERÐAFRÆÐI

Í úttektinni var fyrst og fremst horft til upplýsingatæknideildar Reykjavíkurborgar (UTD), auk þess sem skoðuð voru ýmis atriði er varða aðrar starfseiningar A-hluta Reykjavíkurborgar. Helst var stuðst við ISO/IEC 27001:2013 staðalinn og Skipulagshandbók UTD til að leggja mat á gæði þeirra stýringa sem til staðar eru hjá Upplýsingatæknideild Reykjavíkurborgar.

Við vinnslu skýrslunnar var talað við lykilstarfsmenn og farið yfir ýmis tengd gögn.

HELSTU ÁHÆTTUÞÆTTIR

Vel unnið og reglulegt áhættumat er lykilverkfæri til að átta sig á hversu langt eigi að ganga í hinum ýmsu tilvikum til að tryggja ásættanlega leynd, réttleika og tiltækileika þeirra gagna og kerfa sem eru á ábyrgð borgarinnar.

Einnig þarf að gera strangar kröfur um vandaða forritun, prófanir og uppsetningu til þeirra aðila sem sinna slíkum störfum. Aðrar áhættur tengjast gjarnan ófullnægjandi eftirliti með aðgerðum í kerfum, að mikilvægum öryggisuppfærslum á hugbúnaði sé ekki sinnt, að ytri varnir séu ekki nægjanlega góðar, að ekki sé leitað að óværum í innri kerfum o.s.frv.

HELSTU ÁBENDINGAR

Í framhaldi af úttektinni var bent á nokkur atriði sem standa mætti betur að svo bæta megi netöryggi hjá Reykjavíkurborg:

- **Móttaka nýrra starfsmanna** – Lagt er til að fræðslu um upplýsingaöryggi verði bætt inn í áætlun um móttöku nýrra starfsmanna Reykjavíkurborgar.
- **Fræðsla í upplýsingaöryggi** – Lagt er til að samin verði vitundaráætlun um upplýsingaöryggi fyrir Reykjavíkurborg sem fælist m.a. í að skipuleggja árlega kynningu á upplýsingaöryggi til starfsmanna borgarinnar. Hana mætti gera á vefnum og láta fólk staðfesta áhorf að lestri loknum, eða vera með stutt próf á vefnum.
- **Yfirsýn yfir vefi borgarinnar** – Lagt er til að viðhaldið sé skrá yfir vefi (lén) hjá Reykjavíkurborg þar sem fram koma helstu upplýsingar um þá.
- **Kröfur til birgja** – Lagt er til að í samningum borgarinnar við birgja sem sinna upplýsingatækniþjónustu verði hafður sérstakur viðauki við samninginn þar sem tilgreindar verði þær upplýsingaöryggiskröfur sem borgin gerir til birgja í samræmi við ISO 27001 og ný persónuverndarlög.
- **Trúnaðarmál** – Nokkrar aðrar ábendingar sem máli skipta komu fram en vegna eðlis þeirra flokkast þær sem trúnaðarmál og verða ekki birtar opinberlega.

Skoðað var hvernig UTD uppfyllti kröfur ISO 27001 upplýsingaöryggisstaðalsins og eigin kröfur sem fram koma í Skipulagshandbók UTD.

Úttektir eru oft þess eðlis að í niðurstöðum þeirra eru helst dregnar fram ábendingar um það sem betur mætti fara. Hins vegar er rekstur tölvukerfa og allt sem því tengist risavaxið verkefni. Þótt úttektin hafi leitt í ljós ýmsar ábendingar sem vonandi koma að gagni, þá verður ekki annað sagt en að starfsfólk UTD sé starfi sínu vel vaxið og að það sé vakandi og meðvitað um þær umbætur sem æskilegt væri að fara í. Eins og aðrir þarf UTD að sníða sér stakk eftir vexti og hefur það eflaust áhrif á getu þeirra til að gera eins vel og best væri á kosið.

VIÐBRÖGÐ STJÓRNENDA

Niðurstöður úttektarinnar voru sendar stjórnendum UTD til yfirlestrar og hefur Innri endurskoðun fengið viðbrögð þeirra við þeim ábendingum sem koma fram í skýrslunni. Engar athugasemdir voru gerðar við það sem þar kom fram og í flestum tilfellum ákveðið að bregðast við viðkomandi ábendingu. Í sumum tilfellum bendir UTD réttilega á að ákveðin atriði sem tengjast almennum starfsmönnum borgarinnar sé ekki á þeirra könnu.

Hallur Símonarson
innri endurskoðandi Reykjavíkurborgar