Reykjavíkurborg
Þjónustu- og nýsköpunarsvið

Reykjavík, 14. september 2020
ÞON20080007
R20080151

Til borgarráðs
Ráðhús Reykjavíkur

Efni: Svar við fyrirspurn borgarráðsfulltrúa Sjálfstæðisflokksins um eðli og umfang öryggisveikleika í Hlöðunni.

Vísað er til bréfs, dagsett þann 31. ágúst 2020, þar sem óskað er eftir svari þjónustu- og nýsköpunarsviðs (ÞON) við fyrirspurn borgarráðsfulltrúa Sjálfstæðisflokksins þar sem óskað er eftir upplýsingum um eðli og umfang öryggisveikleika sem fannst í nýju upplýsingastjórnunarkerfi borgarinnar, Hlöðunni.

F.h. þjónustu- og nýsköpunarsviðs,

Óskar J. Sandholt

sviðsstjóri þjónustu- og nýsköpunarsviðs

Hjálagt er svar við fyrirspurn Sjálfstæðisflokksins um eðli og umfang öryggisveikleika í Hlöðunni.

Reykjavíkurborg
Þjónustu- og nýsköpunarsvið

Reykjavík, 14. september 2020
ÞON20080007
R20080151
ÞON
ÓJS

Svar

Viðtakandi: Borgarráð
Sendandi: Óskar J. Sandholt, sviðsstjóri þjónustu- og nýsköpunarsviðs

---

Efni: Svar við fyrirspurn borgarráðsfulltrúa Sjálfstæðisflokksins um eðli og umfang öryggisveikleika í Hlöðunni.

Þann 27. ágúst 2020 lagði borgarráðsfulltrúi Sjálfstæðisflokksins í borgarráði svohljóðandi fyrirspurn:

> *Í fréttatilkynningu frá Reykjavíkurborg, 20. ágúst sl. var greint frá öryggisveikleika í nýju upplýsingastjórnunarkerfi Reykjavíkurborgar. Í tilkynningunni segir: "Við prófanir þann 31. júlí sl. uppgötvuðu sérfræðingar Syndis öryggisveikleika í Hlöðunni sem gerði þeim kleift að komast í gögn og persónuupplýsingar Reykjavíkurborgar og annarra viðskiptavina Hugvits án þess að vera auðkenndur notandi í kerfum Hugvits." Óskað er eftir nákvæmum upplýsingum um öryggisveikleikann og umfang þeirra gagna og persónuupplýsinga sem urðu aðgengilegar án auðkenningar.*

Fyrirspurninni var vísað til umsagnar þjónustu- og nýsköpunarsviðs með bréfi dags 31. ágúst 2020.

Svar:

Upplýsingaöryggisfyrirtækið Syndis var fyrr í sumar falið að gera öryggisskimun á nýju upplýsingakerfi Reykjavíkurborgar, Hlöðunni (GoPro Foris), en vinnsluaðilinn Hugvit ehf. hefur umsjón með kerfinu.

Við skimun Syndis á öryggisveikleikum í Hlöðunni kom í ljós að Hlaðan notaðist við samnýtta þjónustu margra GoPro Foris kerfa óskyldra aðila við gerð PDF skjala (pdf converter). Voru gögn viðskiptavina GoPro hýst á sama stað í skamman tíma hverju sinni, þegar viðskiptavinir virkjuðu þessa tilteknu þjónustu. Kom í ljós að þjónustan var opin út á internetið, án nokkurrar auðkenningar. Syndis sýndi fram á að hægt var að nýta þennan öryggisveikleika til að sækja gögn frá Reykjavíkurborg í þeim tilfellum og á þeim tímapunkti sem verið var að umbreyta skjölum í pdf skjöl. Hugvit hefur girt fyrir veikleikann.

Gagnasafn Reykjavíkurborgar í heild sinni var á engum tímapunkti aðgengilegt óviðkomandi aðilum. Veikleikinn fannst í hliðarvirkni kerfisins, þar sem skjöl flæddu í gegn í pdf umbreytingarferli og voru aðeins í stuttan tíma. Umfang þeirra gagna sem Syndis tókst að komast yfir var því takmarkað.

Syndis hefur farið yfir aðgerða- og atburðasögu, þ.e. log skrár Hugvits, og skoðað hvort óviðkomandi aðilar aðrir en Syndis hafi skoðað eða komist yfir gögnin. Syndis hefur staðfest með nægjanlegri vissu að enginn annar en Syndis hafi nýtt sér veikleikann.

Virðingarfyllst,

Óskar J. Sandholt