Reykjavíkurborg
Þjónustu- og nýsköpunarsvið

Reykjavík, 16. ágúst 2022
ÞON22080027

Til stafrænt ráðs
Ráðhúsi Reykjavíkur

Efni: Gagnagíslataka hjá QuestionPro.

Þann 23. maí 2022 kom upp mögulegur öryggisbrestur hjá framleiðendum og hýsingaraðilum könnunarhugbúnaðarins QuestionPro, en þann 5. ágúst síðastliðinn tilkynnti fyrirtækið að gögn þjónustuþega hefðu verið tekin í gíslingu. Þar á meðal eru tæplega 4.000 netföng starfsmanna Reykjavíkurborgar. Engar vísbendingar eru um að atvikið hafi valdið starfsfólki tjóni og metur öryggisráð skrifstofu upplýsingatækniþjónustu því sem svo að atvikið, sem átti sér stað innan fyrirtækisins QuestionPro, hafi haft lágmarksáhrif á starfsemi borgarinnar.

F.h. Þjónustu- og nýsköpunarsviðs,

Friðþjófur Bergmann,
skrifstofustjóri upplýsingatækniþjónustu Reykjavíkurborgar

Hjálagt:
Minnisblað ÞON22080027 Gagnagíslataka hjá QuestionPro. Reglur um tölvunotkun ÞON21010018. Kynning á netöryggisvörnum og QuestionPro.

Reykjavíkurborg
Þjónustu- og nýsköpunarsvið

Reykjavík, 16. ágúst 2022
ÞON22080027

MINNISBLAÐ

Viðtakandi: Stafrænt ráð
Sendandi: Friðþjófur Bergmann, skrifstofustjóri upplýsingatækniþjónustu

---

Efni: Gagnagíslataka hjá QuestionPro.

Þann 23. maí 2022 kom upp mögulegur öryggisbrestur hjá framleiðendum og hýsingaraðilum könnunarhugbúnaðarins QuestionPro, en þann 5. ágúst síðastliðinn tilkynnti fyrirtækið að gögn þjónustuþega hefðu verið tekin í gíslingu. Þar á meðal eru tæplega 4.000 netföng starfsmanna Reykjavíkurborgar. Engar vísbendingar eru um að atvikið hafi valdið starfsfólki tjóni og metur öryggisráð skrifstofu upplýsingatækniþjónustu því sem svo að atvikið, sem átti sér stað innan fyrirtækisins QuestionPro, hafi haft lágmarksáhrif á starfsemi borgarinnar.

Forsaga:

Þann 23. maí síðastliðinn brutust óprúttnir aðilar í gegnum netöryggisvarnir framleiðanda og hýsingaraðila könnunarhugbúnaðarins QuestionPro sem er gjaldfrjáls (og áskriftar) hugbúnaður til að gera kannanir á internetinu. Náðu árásarmennirnir að taka rúmlega 100 gígabit af gögnum í gíslingu en gögnin fólu meðal annars í sér 22.229.637 netföng, spurningalista og niðurstöður. Af þessum gögnum voru 3.856 netföng með @reykjavik.is endingu.

Þann 5. ágúst, eða um tveimur og hálfum mánuði síðar, stigu forsvarsmenn QuestionPro fram og tilkynntu um gagnagíslatökuna en jafnframt um hótun sem beindist á sama tíma gegn fyrirtækinu um gagnaleka, ef lausnargjald yrði ekki greitt. QuestionPro hefur tilkynnt að fyrirtækið muni ekki greiða lausnargjald en öllum þjónustuþegum fyrirtækisins verði gert viðvart ef að hótun um gagnaleka og þar með öryggisbrestur í starfsemi QuestionPro, raungerist.

Greinargerð:

Helsta hættan af gagnalekum sem þeim er hér um ræðir er sú að tölvuþrjótar noti netföng sem þeir komast yfir til að senda svikapósta. Frá því að tilkynnt var um gagnagíslatökuna þann 5. ágúst síðastliðinn hefur öryggisráð upplýsingatækniþjónustu Reykjavíkurborgar, samkvæmt verklagi, fylgst grant með hvort aukning hafi orðið á rusl- og svikapóstum umfram það sem hefðbundið er. Fram til þessa hefur ekki verið hægt að merkja aukningu og leiða má því líkur að því að tölvupóstnetföng starfsmanna hafi ekki farið í dreifingu.

Reykjavíkurborg
Þjónustu- og nýsköpunarsvið

Þann 10. ágúst 2022 sendi skrifstofa upplýsingatækniþjónustu enga síður viðvörun til starfsfólks Reykjavíkur þar sem upplýst var um mögulegan gagnaleka vegna innbrots hjá QuestionPro. Var starfsfólk beðið að vera á varðbergi gagnvart hugsanlegum svikapóstum og tilkynna þá samstundis. Í sömu andrá var starfsfólk Reykjavíkurborgar einnig minnt á að nýta aðeins hugbúnað sem hefur verið samþykktur af UTR líkt og kemur fram í tölvureglum Reykjavíkurborgar sem samþykktar voru í mannréttinda-, nýsköpunar- og lýðræðisráði þann 7. apríl 2022. QuestionPro hefur ekki verið samþykkt af skrifstofu upplýsingatækniþjónustu sem hugbúnaður til almennrar notkunar innan borgarkerfisins.

Hnippingar (e. nudges) sem þessar eru hefbundið tól sem til þess er gert að minna starfsfólk á að það sjálft gegni mikilvægu hlutverki þegar kemur að því að halda uppi netvörnum í starfsemi borgarinnar. Hnippingar eru skilgreindar sem jákvætt inngrip og sem slíkar eru þær hluti af virkri öryggismenningu.

Mikilvægt er að halda til haga að hver sem er getur skráð sig fyrir notendareikningi hjá QP með hvaða netfangi sem er. Hver sem er getur líka sent könnun á hvaða netfangahóp sem er. Þau tæplega 4.000 Reykjavíkurnetföng sem skráð eru í gegnagrunni QuestionPro geta hafa komið inn í QP kerfið eftir ýmsum leiðum. Vitað er að skrifstofur á einstaka sviðum hafi notað hugbúnaðinn fyrir litlar kannanir sem og stórar. Einnig er ekki hægt að útiloka að starfsfólk borgarinnar og/eða kjörnir fulltrúar hafi mögulega fengið sendar netkannanir úr þessum hugbúnaði frá aðilum utan borgarkerfisins og þar með hafi tölvunetföng þeirra verið vistuð hjá fyrirtækinu.

Niðurlag:

Samkvæmt verklagi rýnir öryggisráð upplýsingatækniþjónustu Reykjavíkurborgar öll frávik sem ógnað geta upplýsingaöryggi hennar. Engar vísbendingar eru um að gagnagíslataka hjá fyrirtækinu QuestionPro og mögulegur gagnaleki hafi valdið tjóni fyrir Reykjavíkurborg og starfsfólk hennar með nokkrum hætti. Metur öryggisráðið því sem svo að atvikið sem átti sér stað hjá QuestionnPro, hafi haft lágmarksáhrif á borgina.

F.h. Þjónustu- og nýsköpunarsviðs,

Friðþjófur Bergmann,
skrifstofustjóri upplýsingatækniþjónustu Reykjavíkurborgar