Reykjavíkurborg
Þjónustu- og nýsköpunarsvið

Reykjavík, 12. janúar 2022

MMS21120233

Til Borgarráðs

Ráðhúsi Reykjavíkur

Efni: Svar við fyrirspurn áheyrnarfulltrúa Flokks fólksins um stöðu öryggismála á Þjónustu- og nýsköpunarsviði – MSS21120233.

Vísað er til bréfs, dagsett 16. desember 2021, þar sem óskað er eftir svörum frá Þjónustu- og nýsköpunarsviði um öryggi á upplýsingatækniinnviðum og hvort öryggisstjóri sé starfandi.

Virðingarfyllst,

fyrir hönd Þjónustu- og nýsköpunarsviðs,

Friðþjófur Bergmann,
skrifstofustjóri upplýsingatækniþjónustu Reykjavíkur

Kjartan Kjartansson,
deildarstjóri stoð- og tækniþjónustu

Loftur Steinar Loftsson ,
deildarstjóri kerfisstjórnar og tæknireksturs

Meðfylgjandi er svar við fyrirspurn Flokks fólksins MMS21120233

Reykjavíkurborg
Þjónustu- og nýsköpunarsvið

Reykjavík, 12. janúar 2022
MMS21120233

SVAR

Viðtakandi: Borgarráð
Sendandi: Friðþjófur Bergmann, skrifstofustjóri upplýsingatækniþjónustu Reykjavíkurborgar, Kjartan Kjartansson deildarstjóri stoð- og tækniþjónustu og Loftur Steinar Loftsson deildarstjóri kerfisstjórnar og tæknireksturs.

Efni: Svar við fyrirspurn áheyrnarfulltrúa Flokks fólksins um stöðu öryggismála á Þjónustu- og nýsköpunarsviði – MSS21120233.

Á fundi borgarráðs þann 16. desember 2021, var lögð fram svohljóðandi fyrirspurn fulltrúa Flokks fólksins, sbr. 62 lið, fundargerðar ráðsins s.d.:

> *Í borgarráði er liður sem heitir óvissustig almannavarna vegna Log4j. Eftir því sem fulltrúi Flokks fólksins kemst næst þá eru hér um að ræða einhverskonar vangaveltur eða kynningar í kjölfar skoðunar öryggismála í netkerfum Reykjavíkur í kjölfar öryggisgallans sem varð vart við um allan heim fyrir nokkrum dögum. Þá er kannski rétt að spyrja hvort það sé búið að yfirfara kerfi borgarinnar hvað þetta varðar. Er ekki einhver sérstakur öryggisstjóri hjá ÞON? Hver er raunveruleg staða öryggismála ÞON / RVK?*

Fyrirspurnin var send Þjónustu- og nýsköpunarsviði til umsagnar með bréfi dagsettu þann 20. desember 2021.

Svar:

Er búið að yfirfara kerfi borgarinnar hvað Log4j varðar?

Þann 24. nóvember 2021 uppgötvaðist öryggisveikleikinn Log4Shell og var hann tilkynntur beint til framleiðanda hugbúnaðar sem nýtir sér JAVA kóðasafnið. Þann 9. desember bárust fyrstu tilkynningar frá alþjóðasamfélaginu um útbreiðslu Log4S öryggisveikleikans og þær alvarlegu afleiðingar sem misnotkun hans gæti haft, sérstaklega þar sem mörg af stærstu upplýsingatæknifyrirtækjum heimsins nýta þetta kóðasafn í hugbúnaði sínum.

10. desember 2021 kl. 09:00 var öryggisráð Þjónustu- og nýsköpunarsviðs formlega virkjað, settur aðgerðarstjóri til að stjórna aðgerðum, neyðaráætlun virkjuð og aðgerðarplan útfært. Haft var samband við alla þekkta birgja sem Reykjavíkurborg hefur samningasamband við og tryggt að unnið væri að því að fyrirbyggja veikleikann og tryggja gögn Reykjavíkurborgar. Sérfræðingar sviðsins voru settir í hæsta viðbragðsstig þar sem ljóst var að vinna þyrfti um þá helgi ásamt að utanaðkomandi sérfræðiaðstoð, sem fengin var til að fara yfir upplýsingatækniumhverfið.

Rætt var á fundi öryggisráðs hvort ástæða væri til að hafa samband við netöryggissveit Fjarskiptastofu en ekki þótti tilefni til þess. Reykjavíkurborg fellur ekki undir skilgreiningu 2.mgr. laga 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða og því er samstarfið við netöryggissveitina ekki náið.

12. desember 2021 þegar fyrstu skönnun var lokið þá var ljóst að upplýsingatækniumhverfi Reykjavíkurborgar var nokkuð vel undirbúið vegna þeirra forvinnu sem hafði þegar verið unnin. Helgin var nýtt til að slökkva á eldri vefsíðum, þjónustum og búnaði sem ekki væri vissa um hvort væru nógu öruggur.

13. desember 2021 kl. 9:00 var fundur aðgerðarstjórnar þar sem farið var yfir aðgerðir helgarinnar og í kjölfarið var ákveðið að hafa samband við öryggisfyrirtækin *Syndis, Secure IT* og *Bithex* til frekari yfirferðar á upplýsingatækniumhverfi Reykjavíkurborgar nú þegar vitað var að hverju þyrfti að leita. Birgjar komu einn af öðrum með skýrslur yfir þær aðgerðir sem þeir höfðu ráðist, en þær veittu fullvissuðu um að í lagi væri með varnir og gögn, út frá öllum þekktum viðmiðunum. Þetta átti við um gögn hvort sem þau væru hýst innan eða utan vélasala Reykjavíkurborgar.

14. desember 2021 var fundur borga víðsvegar um Evrópu á vegum Eurocities þar sem sérfræðingar og þar á meðal sérfræðingar Reykjavíkurborgar báru saman bækur sínar vegna öryggisveikleikans og þar sem deilt var upplýsingum um uppgötvun og aðgerðir. Þátttakendur voru sammála um að styrkja enn frekar samstarfið á sviði öryggismála í upplýsingatækni og deila þekkingu, reynslu og gögnum.

15. desember 2021 er haldið áfram ítarlegri aðgerðum við skoðun ásamt eftirliti til að fylgjast með ef verður vart við óðeðlilega netumferð í upplýsingatækniumhverfinu. Þessi vinna mun halda áfram næstu vikurnar til tryggja umhverfið. Stjórnendur og sérfræðingar Þjónustu- og nýsköpunarsviðs telja að þessar aðgerðir sem ráðist hefur verið í hafi skapað borginni vel viðunandi stöðu en það er sagt með þeim fyrirvara að ávallt getur eitthvað komið upp sem krefjist mjög skjótra viðbragða.

Vöktun hefur haldið áfram til dagsins í dag í samstarfi við umrædd öryggisfyrirtæki, aðrar stofnanir og borgir.

Er ekki einhver sérstakur öryggisstjóri hjá ÞON?

Deildarstjóri kerfisstjórnar og tæknireksturs hefur hlutverk öryggisstjóra til að tryggja rekstrarsamfellu upplýsingatækniinnviða Reykjavíkurborgar og nýtur hann liðsinnis fremstu öryggisfyrirtækja í upplýsingatækni hér á landi. Skrifstofustjóri upplýsingatækniþjónustu Reykjavíkur sinnir ISO27001 stjórnkerfis upplýsingaöryggis.

Í skipulagsbreytingum á skrifstofu upplýsingatækniþjónustu Reykjavíkurborgar (UTR) sem komu til framkvæmda annarsvegar á árinu 2019 og hins vegar á árinu 2020 voru hlutverkum og verkefnum breytt og þau flutt milli ábyrgðaraðila. Ábyrgð gæðamála var flutt á skrifstofu sviðstjóra ÞON til að stýra gæðum þvert á skrifstofur ÞON. Skrifstofustjóra upplýsingatækniþjónustu Reykjavíkur var falin sú ábyrgð að viðhalda gæðaskjölum og gæðamenningu fyrir sína starfsemi og hafa umsjón með ISO 27001 stjórnkerfi upplýsingaöryggis á vettvangi Öryggisráðs UTR.

Öryggisráð er stýrihópur ISO27001 stjórnkerfis upplýsingatækniþjónustu. Í öryggisráði sitja stjórnendur skrifstofu upplýsingatækniþjónustu ásamt öryggishönnuði. Haldnir eru mánaðarlegir fundir um rekstur stjórnkerfisins og þar er farið yfir; niðurstöður innri og ytri úttekta, skráð öryggisfrávik og hvort rekstrarfrávik hafi ógnað upplýsingaöryggi. Út frá áhrifum og umfangi frávika er ráðist í rótargreiningar og stofnað til úrbótaverkefna. Rýnt er í öryggisógnir sem gætu staðið að upplýsingatækniumhverfinu ásamt því að setja fram umbótaverkefni í því sambandi.

Skrifstofustjóri upplýsingatækniþjónustu leiðir öryggisráð sviðsins og þar eiga einnig sæti upplýsingatæknihönnuðir UTR. Deildarstjóri kerfisstjórnar og tæknireksturs var falin sú ábyrgð að viðhalda rekstraröryggi á upplýsingatækniinnviðum Reykjavíkurborgar.

Hver er raunveruleg staða öryggismála ÞON / RVK?

Tölvuumhverfi borgarinnar hvílir í dag á nokkuð traustum grunni, ekki síst í kjölfar þess átaks í stafrænni umbreytingu sem sett var af stað í tengslum við Græna plan borgarinnar. Þannig hefur umtalsverðu fjármagni þegar verið ráðstafað í uppbyggingu upplýsingatækniinnviða Reykjavíkurborgar og vegna þeirrar fjárfestingar var þegar búið að vinna ákveðna grunnvinnu sem gerir það að verkum að upplýsingatækniumhverfi borgarinnar er betur í stakk búið til að takast á við öryggisveikleikann í dag en áður fyrr.

Sú stefnubreyting og áhersla að framleiðsla hugbúnaðarlausna sé samræmd og stýrt í þróunar- og prófunarumhverfi UTR hefur augljósa kosti þegar upp koma veikleikar sem þessi. Þá liggur fyrir frá upphafi uppruni þess kóða sem notaður er innan töluumhverfisins. Mest ógn stafar af veikleikum sem þessum í lausnum sem ytri aðilar hafa sérsmíðað eða aðlagað og hýstar eru innan tölvuumhverfis borgarinnar. Þær lausnir þarf að prófa gagnvart veikleikum sem finnast og vakta sérstaklega.

Tæpur áratugur er síðan hafist var handa við að sameina umsýslu, innkaup og rekstur á upplýsingatækniinnviðum borgarinnar á einni miðlægri skrifstofu upplýsingatækniþjónustu Reykjavíkurborgar. Þeirri vinnu er ekki alveg lokið og enn má finna einingar innan borgarkerfisins sem sýsla með og kaupa inn upplýsingatækniinnviði án aðkomu Þjónustu- og nýsköpunarsviðs. Þetta gerir það að verkum að skrifstofa upplýsingatækni á Þjónustu- og nýsköpunarsviði hefur ekki yfirsýn að öllu leyti yfir hvaða hugbúnaður er í notkun eða hvar gögn eru geymd. Vegna þessa er örðugra en ella að tryggja heildarvarnir fyrir borgina og takmarkast því neðangreind vinna við þekkta upplýsingatækniinnviði sem eru á forræði skrifstofu upplýsingatækniþjónustu Reykjavíkurborgar á Þjónustu- og nýsköpunarsviði.

Öryggisfyrirtækið Syndis var fengið þann 26. október 2021 til að gera úttekt á öryggi upplýsingatækniinnviða bæði á ytra og innra umhverfi borgarinnar. Í framhaldi var rekstrarráð UTR kallað saman og farið var í umfangsmiklar umbótaaðgerðir í uppfærslum á stýrikerfum, gagnagrunnum og hugbúnaði yfir í nýjustu útgáfur. Upplýsingaskrifstofa Reykjavíkurborgar hefur einnig verið með samning við öryggisfyrirtækið Bithex sem skannar reglulega vefsíður Reykjavíkurborgar sem eru í rekstri hjá UTR og út úr þeirri yfirferð er síðan farið í umbótaaðgerðir.

Þann 9. nóvember 2021 var haft samband við sænska öryggis- og upplýsingatæknihönnunar fyrirtækið 1o.se með beiðni um að skanna allt sem tengist innra neti Reykjavíkurborgar, hvar

sem gögn eru hýst, í vélasölum Reykjavíkurborgar og hjá birgjum innanlands eða í skýjaþjónustum. Þannig næst skýrari heildarmynd af núverandi upplýsingatækniumhverfi Reykjavíkurborgar og er það grunnurinn að framtíðarhögun á enn öruggari og áreiðanlegri upplýsingatækniinnviðum, í takti við þarfir framtíðarinnar, sem hægt verður að stjórna á einfaldan og skilvirkan hátt. Verkefnið er hafið og nær fullum þunga á fyrsta árshluta 2022.

Í september 2020 tók gildi fjarskiptastefna Íslands til 15 ára og 5 ára fjarskiptaáætlun sem liður í framkvæmd þjóðaröryggisstefnu landsins. Eru þetta fyrstu heildarlögin um netöryggi hérlendis sem byggjast á netöryggistilskipunum ESB. Sett er fram það megin markmið að örugg nýting upplýsingatækni verði ein meginstoð hagsældar á Íslandi, nýting sem byggist jafnframt á mannréttindum, persónuvernd og frelsi til athafna.

Í netöryggisráði eiga sæti fulltrúar ráðuneyta og stofnana sem koma að netöryggismálum með ýmsum hætti og þurfa því að skiptast á upplýsingum og eiga samstarf þar sem ábyrgð og eftirlit dreifist jafnframt á þá. Reykjavíkurborg fellur í lögunum eins og fyrr segir ekki undir skilgreininguna “mikilvægir innviðir” en borgin er þó sá opinberi aðili sem rekur umfangsmesta upplýsingatækniumhverfi landsins, og er því veigamikill aðili að grunn innviðum þess. Borgin vegur einnig þungt þegar kemur að stöðu og ásýnd Íslands í netöryggismálum almennt en gíslataka á kerfum borgarinnar hefði bein og ótvíræð áhrif á 1/3 hluta þjóðarinnar.

Frá stofnun Þjónustu- og nýsköpunarsviðs árið 2019 með tilheyrandi skipulags- og áherslubreytingum hjá UTR og vegna fjárfestinga Græna plansins hefur verið unnið markvisst að því að styrkja varnir upplýsingatækniumhverfis Reykjavíkurborgar og mun sú vinna halda áfram til að ná markmiðunum að vera með eins örugga og áreiðanlega upplýsingatækniinnviði og hægt er auk þess að ná að stjórna á þeim einfaldan og skilvirkan hátt. Haldið verður áfram með þessa vinnu af fullum þunga inn í næsta ár þar sem staða á upplýsingatækniumhverfinu og framtíðarhögun þess verður enn ljósari þá.

Því skal þá haldið til haga að ekki er hægt að tryggja fullkomlega tæknilegar öryggisráðstafanir þannig að hægt verði að koma alfarið í veg fyrir upplýsingaleka eða gagnagíslatöku, því er þörf á stöðugri ítrun þegar kemur að uppfærslu öryggis í upplýsingatækniumhverfi borgarinnar svo halda megi í við þróunina með nýjungum og mæta netglæpum af krafti.

Reykjavíkurborg
Þjónustu- og nýsköpunarsvið

Fyrir hönd Þjónustu- og nýsköpunarsviðs,

Friðþjófur Bergmann
Skrifstofustjóri upplýsingatækniþjónustu Reykjavíkur

Kjartan Kjartansson
Deildarstjóri stoð- og tækniþjónustu

Loftur Steinar Loftsson
Deildarstjóri kerfisstjórnar og tæknireksturs