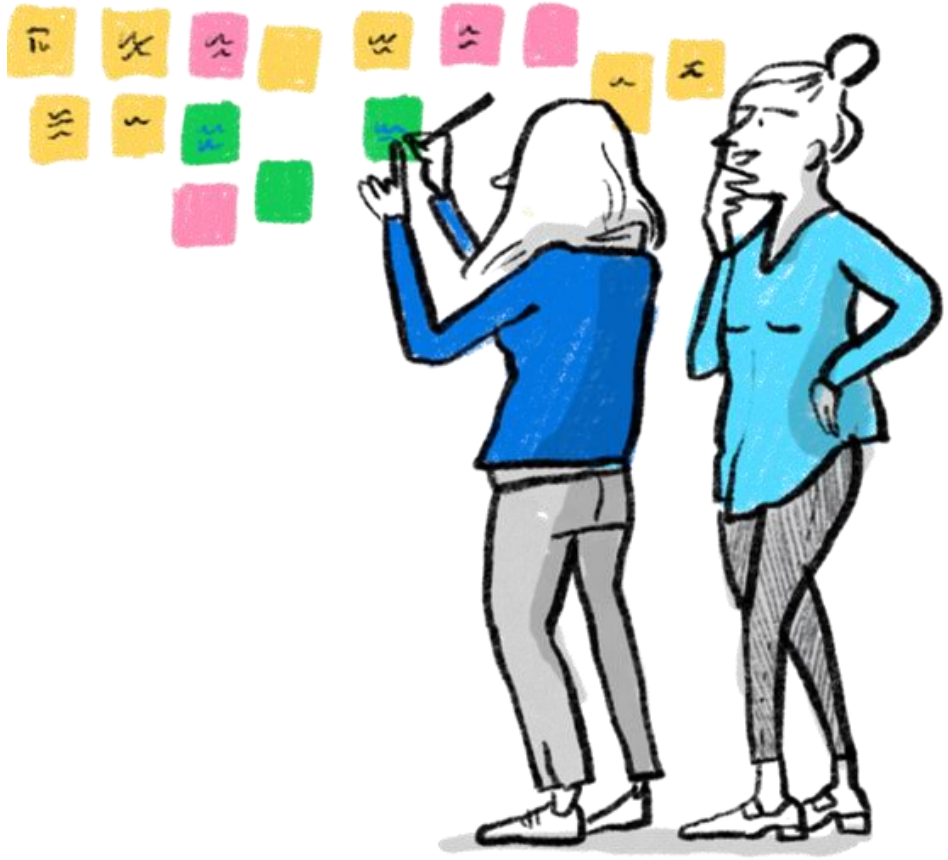
Question PRO gagnaleki

Netöryggisvarnir Reykjavíkurborgar

Friðþjófur Bergmann

Question Pro könnunarhugbúnaður



Maí 2022

- Gagnagíslataka hjá framleiðendum og hýsingaraðilum könnunarhugbúnaðarins á 22 milljónum netfanga, spurninga og niðurstöðum kannana
- 3.856 netföng eru með @reykjavik.is endingu

Ágúst 2022

- Aðvörun sett á Workplace, innri samkiptamiðil borgarinnar, um hugsanlega fjölgun ruslpósta í innhólfi í tölvupósti.

Ábyrgð borgarinnar

- Gagnalekinn er ekki öryggisbrestur á upplýsingatækniinnviðum Reykjavíkurborgar, heldur hjá Question Pro.
- Hugbúnaðurinn er ekki samþykktur né stjórnað af upplýsingatækniþjónustu borgarinnar.

- Gagnalekar eru óumflýjanlegir í nútímasamfélagi
- Markmið Reykjavíkurboargar er að takmarka eftir fremsta megni skaðann sem af þeim getur hlotist

Netárásir á Reykjavíkuraborg

- Síðastliðin 5 ár hafa verið gerðar um 17.000 tilraunir til að komast í gegnum öryggisnetvarnir borgarinnar
- Skilgreind voru um 2.000 atvik til viðbótar þar sem óværur eða svikapóstar komust í gegnum eldveggi
- Ein árás hefur leitt til kæru

- Helstu flokkar árása eru: netveiðar (e. phishing), spilliforrit (e. maleware og ransomeware) svo og Ddos álagsárásir.

Netárásir og þróun þeirra

- Fjöldi netárása fjölgaði um 80% um allan heim á tímum Covid-19 (e. cyberpandemic).
  - Dæmi: Google blokkaði daglega tæplega 20 milljón Covid-19 tengdra svkikapósta, á fyrstu 6 mánuði bylgjunnar.
- Á sama tíma fækkaði árásum þar sem aðilar komust í gegnum eldveggi um 20% hjá Reykjavíkurborg.

Varnir borgarinnar

- Í gegnum fjárfestingu Græna plansins hefur verið hægt að hraða uppfærslu upplýsingatækniinnviða borgarinnar með margvíslegum hætti:
    - Dæmi um aðgerðir: innleiðing Identity Service Engine öryggiskerfis, Security Operation Center öryggisvöktun, QRadar - Security Information and Event Management netvöktunarkerfi, BitLocker dulkóðun á tölvur, öryggisafritun gagna, Siteimprove gæðastýring á vefi, eldveggir uppfærðir, sjálfvirk læsing á netskápa, skýjaþjónustur innleiddar og vél- og hugbúnaður lagður niður, fjölþátta auðkenning og breyttar aðgangsstýringar, DDI stjórn- og öryggiskerfi, DataDog eftirlitskerfi.
    - Dæmi um reglubundið eftirlit: Gæða- og öryggisvottun ISO27001, úttektir Innri endurskoðunnar á netöryggi borgarinnar framkvæmdar á 2 ára fresti, frumkvæðisathuganir UTR í samstarfi við r´ðagjafafyrirtæki.
- Netöryggissamstarf innanlands: Netöryggissveit CERT-IS, Syndis, fjölmargir birgjar.
- Netöryggissamstarfs utanlands: Gartner, Eurocities,

Framtíðarhögun upplýsingatækniinnviða

- Síðustu misseri hafa verið gerðar viðamiklar breytingar á upplýsingatækniinnviðum borgarinnar til að bæta upplýsingaöryggi.
- Meðan þróun netárása heldur áfram þarf að byggju upp og uppfæra varnir borgarinnar
- Nýlega var samið við KPMG í kjölfar útboðs um hönnun framtíðarumhverfis fyrir upplýsingatækniinnviði Reykjavíkurborgar svo tryggja megi enn umhverfi sem hægt er að stjórna á einfaldan og skilvirkan hátt

Reykjavík