Öryggi upplýsingartæknikerfa

Skilgreining árásarflata

UTR hefur skilgreint mögulega árásarfleti og aukið varnir á eftirfarandi stöðum:

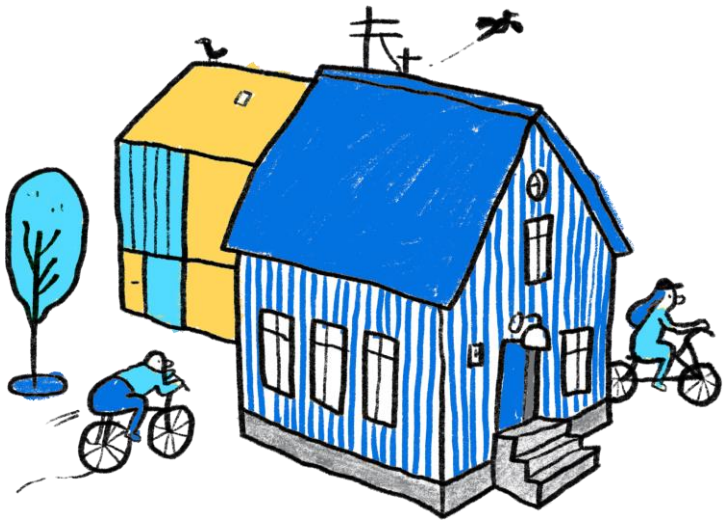
- Notandinn
- Staðbundin upplýsingakerfi (gögn vistuð í tölvusal Borgartúni)
- Kerfi og gögn vistuð í tölvuskýjum
- Skýjalausnir
- Vefir
- Netkerfi og samtengingar

Notandinn

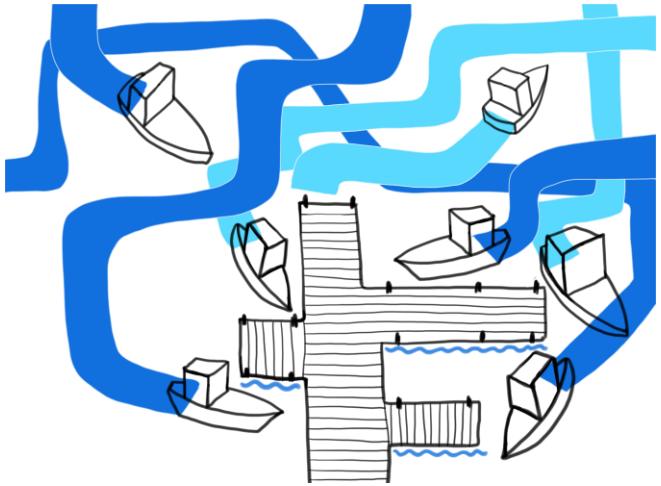
- Samræmdar varnir með notkun á Defender lausnamenginu frá Microsoft
- Margþátta auðkenningar virkjaðar alls staðar þar sem því er viðkomið
- Innleitt kerfi til að takmarka að notendur séu með aukin réttindi á eigin tölvur
- Aukin fræðsla fyrir notendur um ýmsa þætti er snúa að uplýsingaöryggi – útboð vegna fræðsluefnis framundan
- Qradar eftirlitskerfi í notkun til að fylgjast með óvenjulegum aðgerðum eða atvikum í kerfum okkar
  - Þegar óeðlilegar aðgerðir eru greindar koma til sjálfvirkar aðgerðir, s.s. að loka aðgangi tímabundið, senda viðvörun eða óska eftir að notandi auðkenni sig.

Staðbundin kerfi og gögn

- Varnir gegn álagsárásum til staðar til að draga úr áhrifum ef slíkar árásir eru gerðar á þau kerfi sem eru vistuð í tækjasal í Borgartúni
  - Ekki vitað til að reynt hafi á þessar varnir
- Eftirlit með búnaði
- Útboð til að útvista vistun gagna í tækjasal Reykjavíkur í Borgartúni fyrirliggjandi
- Afritun útvistað, m.a. til að bregðast við áhættu vegna gagnagíslatöku
- Qradar eftirlitskerfi í notkun til að fylgjast með óvenjulegum aðgerðum eða atvikum í kerfum okkar.
- Unnið að forgangsröðun og flokkun kerfa eftir mikilvægi. Þessi flokkun er unnin í samráði við eigendur og ábyrgðaraðila kerfa borgarinnar.
- Rafstöð Ráðhúsi nýlega skipt út og er reglulega yfirfarin.



Kerfi og gögn vistuð í tölvuskýjum



- Samræmdar varnir með notkun á Defender lausnamenginu frá Microsoft
  - Á seinustu 4 vikum lokaði Defender fyrir ca 79.200 mismunandi tilraunir til árása í Microsoft umhverfi okkar.
- Qradar eftirlitskerfi í notkun til að fylgjast með óvenjulegum aðgerðum eða atvikum í kerfum okkar
- Skilgreindar kröfur Reykjavíkurborgar um öryggi þeirra tölvuskýja sem eru notuð og staðfestingar að þau tölvuský mæti lagalegum og tæknilegum kröfum borgarinnar

Skýjalausnir

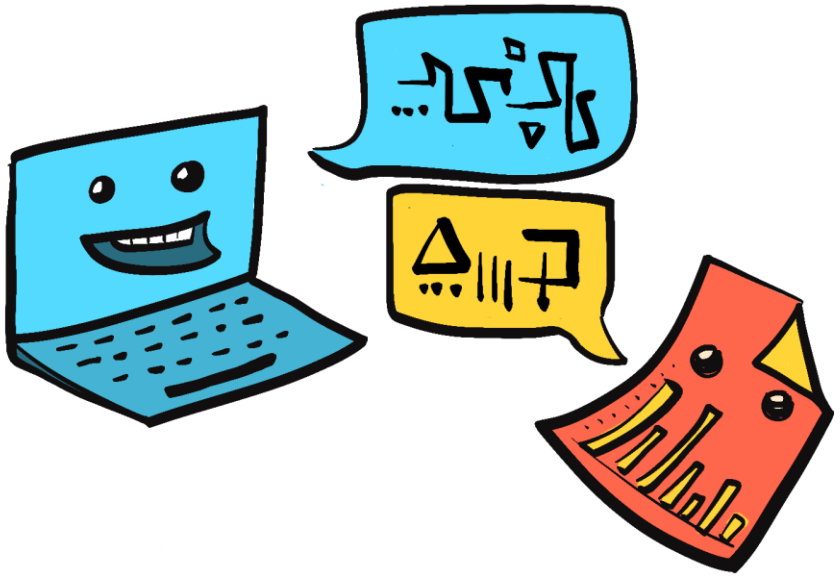
- Stefnumiðuð notkun á skýjalausnum (SaaS) til að leysa verkefni notenda
- Skilgreindar kröfur Reykjavíkurborgar um öryggi þeirra skýjalausna sem eru notuð og staðfestingar að þær lausnir mæti lagalegum og tæknilegum kröfum borgarinnar
- Samræmdar varnir með notkun á Defender lausnamenginu frá Microsoft
- Qradar eftirlitskerfi í notkun til að fylgjast með óvenjulegum aðgerðum eða atvikum í kerfum okkar

Vefir

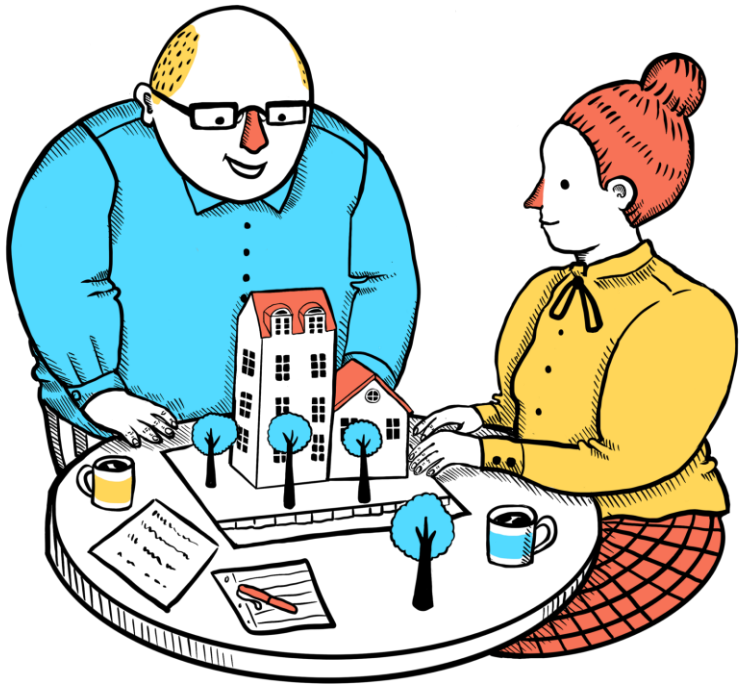
- Vefir á vegum borgarinnar eru mismunandi. Vefir hafa verið flokkaðir eftir mikilvægi og áhrifum ef viðkomandi vefur fer niður
- Mikilvægir vefir eru varðir fyrir álagsárásum auk þess sem frekari stýringar eru meðal annars til staðar varðandi breytingar á vefum
  - Ekki vitað til að reynt hafi á þessar varnir
- Aðrir vefir sem ekki eru skilgreindir sem mikilvægir eru varðir í samræmi við mikilvægi
- Reglulegar veikleikaprófanir á vefum
- Qradar eftirlitskerfi í notkun til að fylgjast með óvenjulegum aðgerðum eða atvikum í kerfum okkar

Netkerfi og samtengingar

- ISE kerfi notað til að tryggja að einungis réttir aðilar fái aðgang að kerfum og gögnum innan kerfa Reykjavíkurborgar
- Umbrella kerfið fylgist með netumferð og lokar fyrir óæskilega umferð um leið og tilraunir koma til að reyna að tengjast.
  - Seinustu 30 daga hefur Umbrella kerfið samtals lokað fyrir um 8000 öryggisógnir (ca. 3000 tilraunir til óværusmita,4200 tilraunir til rafmyntamisnotkunar, 120 svikatilraunir).
- Qradar eftirlitskerfi í notkun til að fylgjast með óvenjulegum aðgerðum eða atvikum í kerfum okkar.
- Nýlegt útboð á rekstri netkerfis, uppfærslur á búnaði og heildaryfirferð stillinga.



Alltumlykjandi ráðstafanir



- Stjórnkerfi upplýsingaöryggis samkvæmt ISO 27001 hefur verið starfrækt hjá UTR frá 2015. Það stjórnkerfi er nauðsynlegur þáttur í skipulagi varna og ráðstafana sem eru til staðar hjá borginni.
  - Umræður hafa verið um að innleiða einnig slíkt stjórnkerfi hjá öðrum sviðum borgarinnar. Umræður við SFS eru þar komnar lengst. (Nánar um ISO 27001 á næstu glæru)
- Qradar eftirlitskerfi er tengt við öll kerfi borgarinnar og notast við gervigreind til að greina óvenjuleg atvik og aðgerðir. Þegar mannleg aðkoma er nauðsynleg eru sendar tilkynningar í verkbeiðnakerfi borgarinnar.
- Heildræn stefna til staðar um upplýsingatækni hjá borginni. Stefnt á einsleitt og samræmt umhverfi þar sem samræmdar lausnir virka alls staðar.
- Yfirferð og rýni á neyðar- og viðbragðsáætlunum.
  - Skilgreining leikbóka til að bregðast við ákveðnum aðstæðum.

ISO 27001 stjórnkerfi upplýsingaöryggis

- Stjórnkerfi upplýsingaöryggis samkvæmt ISO 27001 skilgreinir hvernig takast ógnir og auka öryggi
- Helstu verkfæri stjórnkerfisins eru áhættumat, innri úttektir og rammi til að takast á við atvik sem upp munu koma
- Úttekt fer fram árlega, en þriðja hvert ár er skírteini endurútgefið
- Í hverri úttekt koma fram ábendingar og athugasemdir sem eru skráðar í Jira og leystar eins og önnur verkefnis sviðsins
- Taka þarf ákvörðun um hvort útvíkka eigi vottað stjórnkerfi til annarra sviða

Úttektir og aðhald innri endurskoðunar

- Innri endurskoðun og ráðgjöf framkvæmir reglulega úttektir á störfum UTR
- Seinustu úttektir eru:
  - Aðgangsstýringar tölvukerfa
  - Rekstrarsamfella (snýr að kerfum UTR og FAS)
  - Netöryggi
- Ábendingar IER eru fjölbreyttar og snúa að flestum þáttum reksturs UTR
  - Þegar um umbótaverkefni er að ræða eru þau verkefni meðhöndluð eins og önnur verkefni sviðsins
  - Úttektir IER hafa verið mjög gagnlegar og málefnalegar

Sérstakar ráðstafanir vegna leiðtogafundar

- Við erum alltaf tilbúin að takast á við aðsteðjandi ógnir, líka fyrir svona uppákomur
  - Í aðdragandi yfirförum við þær ráðstafanir sem við erum með og förum yfir ferlana okkar
  - Við ræðum við okkar birgja/þjónustuaðila og tryggjum að við séum öll á sömu blaðsíðunni
  - Við höfum fengið upplýsingar frá Ríkislögreglustjóra og CERT-ÍS varðandi undirbúning og mögulegar áhættur
  - Við höfum sent tilkynningar til notenda um að vera vel á verði gagnvart ógnum
- Sérstakt eftirlit verður með reykjavik.is og viðbragð skilgreint ef tekið er eftir mögulegum árásum á þá vefsíðu
- Öryggi og upplifun notenda berjast oft um hvort skuli fá meira vægi. **Næstu vikur mun öryggi kerfa og upplýsinga skipta mestu máli.** Það getur þess vegna verið að notendur muni upplifa einhver óþægindi eða hægagang í kerfum. Staðan verður endurskoðuð eftir fundinn nema aðstæður verði algerlega óásættanlegar fyrir notendur

Reykjavík