

Landupplýsingar undir öryggislinsu

Trúnaður, réttleiki og tiltækileiki - og hvað þeir þýða fyrir rekstur kerfanna sem vinna með gögnin.

Jón Kristinn Ragnarsson
jon.kristinn.ragnarsson@reykjavik.is

DÆMI ÚR RAUNVERULEIKANUM

Ferðamenn slógu „Geysir“ inn í GPS - og enduðu fastir í snjó fastir í snjó uppi við Heklu.

Gögnin litu rétt út en leiddu þá á rangan og hættulegan stað. Bíllinn festist og það voru bændur á svæðinu sem fundu þá.

Ekkert af þessu er tölvuárás. Samt er þetta öryggisatvik.

GÖÐSÖGNIN

„Gögnin okkar eru opin - upplýsingaöryggi kemur kemur okkur lítið við.“

Það stenst ekki. Fyrir landupplýsingar er stærsta áhættan sjaldnast lekinn - heldur að gögnin séu röng eða ekki til staðar þegar á reynir.

NÁLGUNIN

Sama linsan, önnur forgangsöröð

01 • Réttleiki

GOÐ NÝ NÖÐ ÖPPÉ

Integrity - áreiðanleiki og rekjanleiki gagnanna.

02 • Tiltækileiki

Eru gögnin til staðar?

Availability - aðgengi þegar á þarf að halda.

03 • Leynd

Réttir aðilar með aðgang?

Confidentiality - mikilvæg, en ekki alltaf efst.

Réttleiki og tiltækileiki fyrst. Leyndin síðast - en ekki síst.

Eru gögnin rétt?

Röng hnit og blönduð viðmiðunarkerfi (ISN93, ISN2016, WGS84) líta sakleysislega út en leiða til rangra ákvarðana - í skipulagi, viðbragði og framkvæmdum. Vörnin er rekjanleiki, útgáfustýring og ritstýrð vinnuferli.

GERVIGREIND

Sífelld meira af gögnum er leitt út með líkönum í stað þess að vera mælt. Er flöturinn mældur eða ágískaður - og sést sú óvissa í lýsigögnunum?

Eru gögnin til staðar?

Kortapjónustur liggja undir 112, veitum, samgöngum og náttúruvárvöktun. Þegar þjónusta dettur út í eldgosi eða flóði er það innviðabrestur, ekki tæknilegt smáatriði. Vörnin er uppitímamarkmið, offramboð og skýr birgjastýring.

GERVIGREIND

Nýr hlekkur í gagnakeðjunni sem getur fallið út eða takmarkast - en sama tækni styrkir líka tiltækileika og réttleika með sjálfvirkri vöktun og frávikagreiningu.

Réttir aðilar með aðgang?

Opin gögn þýða ekki að allt sé opið: viðkvæmir innviðir, persónugreinanleg staðsetning og samþjöppun annars saklausra gagnasetta geta afhjúpað það sem ekki átti að sjást.

GERVIGREIND

Um leið og viðkvæm gögn fara inn í ytri gervigreindarþjónustu tapast stjórn - undirvinnsluaðilar, gagnastaðsetning, GDPR. Og líkön geta ályktað mynstur sem gögnin sýndu ekki berum augum.

Úr CIA í rekstrarkröfur

Þáttur	Rekstrarkröfur
Réttleiki	Gagnagæði, lýsigögn, útgáfu- og breytingastjórnun, ritaðgangur
Tiltækileiki	Uppitímamarkmið, RTO/RPO, afritun og endurheimt, rekstrarsamfella
Leynd	Gagnaflokkun, aðgangsstýring, persónuverndarmat (DPIA)
Gervigreind	Mannlegt eftirlit, gagnsæi, EU AI Act, útvíkkað persónuverndarmat

Gervigreind bætir kröfum ofan á þær hefðbundnu - hún kemur ekki í staðinn fyrir þær.

SÝNIDÆMI

Eitt gagnasett, flokkað

Lagnakort veitu - vatn og fráveita

Réttleiki

Hátt

Tiltækileiki

Hátt

Leynd

Miðlungs

Ritstýrð uppfærsla og rekjanleiki, hátt uppitímamarkmið með afritun, og takmarkaður aðgangur að nákvæmri legu.

Flokkunin ræður kröfunum - ekki tilfinningin.

Landupplýsingar eru innviðir.

Flokkið

Gefið gögnunum CIA-einkunn.

Metið

Leiðið rekstrarkröfurnar af einkunninni.

Bregðist við

Gerið viðbragðsáætlun áður en á reynir.

SPURNINGAR?

Takk fyrir.

Jón Kristinn Ragnarsson

Upplýsingaöryggishönnuður og ráðgjafi