



Tveir heimar netöryggis

Arnaldur F. Axfjörð, verkefnastjóri öryggismála
Miðstöð rafrænna heilbrigðislausna/embætti landlæknis

Hver hækkar netöryggisstig Íslands? Á ég að gera það?

Ráðstefna Fjarskiptastofu um netöryggismál - Hilton Nordica, 18. október 2023



















Hvers vegna er þetta svona mikilvægt?

Embætti landlæknis

Mikilvægir innviðir samfélagsins

- Sviðsmyndir netöryggis eru í raun tvær
 - Dags-daglegi heimurinn og áfallaheimurinn
- Megin markmið í stjórnun netöryggis er að lágmarka líkur á því að verða fyrir áföllum
 - Ávallt þarf þó að vera með viðbúnað ef illa fer
- Það þarf að efla getu net- og upplýsingakerfa til að standast hvers konar ógnir
 - Áhersla á aðgengi að sannvottuðum uppruna, heilleika og trúnaði gagna og tengdrar þjónustu
- Markmið öryggisráðstafana verður að vera að lágmarka hættu á áföllum
 - Efla viðnámsþrótt net- og upplýsingakerfa í dags-daglegri starfsemi
 - Áherslan þarf að vera á getu kerfa til að standast fyrirsjáanlegar ógnir



Hvers vegna er þetta svona mikilvægt?

Embætti landlæknis

Mikilvægir innviðir samfélagsins

- Ekkert svið samfélagsins er eyland – það þarf samvinnu
 - Vettvang fyrir upplýsingamiðlun og samhæfingar með ásýnd á stöðu netöryggis í samfélaginu á hverjum tíma
 - Vinna markvisst að því að efla viðnámsþrótt net- og upplýsingakerfa mikilvægra innviða byggt á skírri sýn á stöðumynd áhættu á hverjum tíma
 - Þarf aðkomu lykilaðila sem hafa afgerandi snertiflöt við öryggi net- og upplýsingakerfa mikilvægra innviða
- Ef áfall verður, þá þarf að grípa til aðgerða til að lágmarka skaða og endurreisa gögn og þjónustu hið fyrsta
 - Þá þarf samstillingu viðbragðsaðila, þ.m.t. Netöryggissveitarinnar, almannavarna, varnarmál og löggæslu



Framsetning hjá NIST (*cybersecurity resilience*)

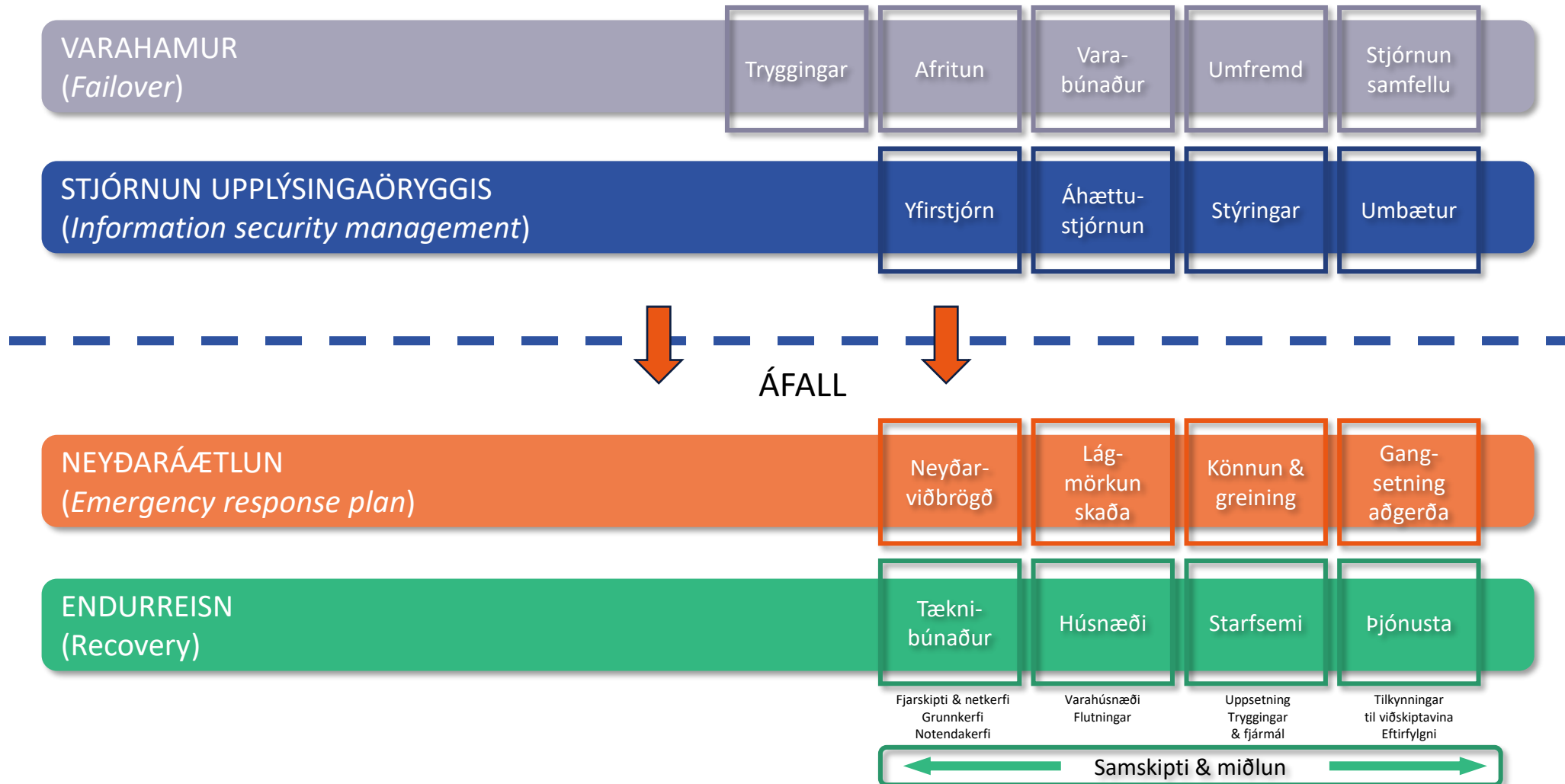
- **Þekkja** (e. identify) – stjórna áhættu í netöryggi (kerfi, fólk, gögn, hæfni, önnur verðmæti)
 - **Vernda** (e. protect) – ráðstafanir til að tryggja afhendingu mikilvægrar þjónustu
 - **Skynja** (e. detect) – bera kennsl á netöryggisatburði
-
- **Bregðast við** (e. respond) – grípa til aðgerða vegna netöryggisatvika sem koma upp
 - **Endurreisa** (e. recover) – viðhafa áætlanir fyrir viðnámsþrótt og til að endurreisa hvaða virkni eða þjónustu sem varð skert vegna netöryggisatviks



Heimarnir tveir!

Embætti landlæknis

REKSTUR (dags-dagleg starfsemi)





Stjórnun rekstrarsamfelli – viðbúnaður fyrir áföll

Embætti landlæknis

NEYÐARÁÆTLUN (ÁÆTLUN UM NEYÐARVIÐBRÖGÐ)

NEYÐARVIÐBÚNAÐUR (VIÐBÚNAÐARÁÆTLUN)
(Fyrirbyggjandi aðgerðir)

VIÐBRAGÐSÁÆTLANIR
(Leiðréttandi aðgerðir)

Fyrstu viðbrögð

Eftirfylgni

Aðgerðaráætlanir

Bilun í upplýsingavinnslu

Eldsvoði

Loftmengun

Sjúkdómafaraaldur

Árás á starfstöð

Skaði á starfsaðstöðu

Jarðskjálfti

Árás á upplýsingar

{Önnur vá}

ENDURREISNARÁÆTLANIR

ENDURREISN UPPLÝSINGAVINNSLU

Endurreisn
samskipta

Endurreisn
grunnkerfa

Endurreisn
notendakerfa

ENDURREISN Á STARFSEMI

Endurreisn
húsnæðis

Endurreisn ferla

Endurreisn
þjónustu



Lykilþættir í eflingu viðnámsþróttar mikilvægra innviða

- Skír og sameiginleg stefna og meginreglur (e. principles) í netöryggi.
 - Góð og skír sýn á áhættu og öryggisstýringar á hverjum tíma
 - Vettvangur fyrir upplýsingamiðlun og samhæfingu aðgerða í þróun og uppbyggingu
-
- Innviðir eru mikið til sameiginlegir og þurfa að vera samvirkir
 - Það er ekki nóg að hugsa bara um aðgerðir til að bregðast við áföllum



Öryggi og traust byggir á sameiginlegum innviðum sem styðja netöryggi

- Þekking og vitund í samfélaginu um netöryggi – og virðing fyrir mikilvægi þess
- Traustþjónusta
 - Auðkenning og undirritanir séu í samræmi við eIDAS
 - Útfærsla sem tryggir viðunandi réttaráhrif í samræmi við mat á áhættu og áhrifum skaða
- Vottorð
 - Viðunandi styrkleiki (eSeal/eIDAS) í samræmi við kröfur
 - Sannvottanleg, óhrekjanleg og hægt að afturkalla
- Umboð
 - Byggð sem vottorð – sannvottanleg, óhrekjanleg og hægt að afturkalla
 - Grunngerð og samræming sem geri ráð fyrir mörgum útgefendum og mörgum treystendum



Öryggi og traust byggir á sameiginlegum innviðum sem styðja netöryggi

- Áreiðanleg gögn og viðurkenndar gagnaveitur
 - Staðfesting gagna byggð á sannvottun frá upprunaaðila (e. authentic data)
 - Veitendur gagna (t.d. úr opinberum skrá) séu áreiðanlegir (e. authorized source)
- Áreiðanleg samskipti og traust í miðlun gagna
 - Gegnsætt varðandi sértækar kröfur; hægt að staðfesta að kröfur séu uppfylltar
- Traust til miðlægrar kerfisþjónustu, t.d. sannvottunarþjónustu
 - Uppfylli kröfur nauðsynlegrar þjónustu mikilvægra innviða
- Traust byggt á kröfum um útfærslu kerfa, rekstur þeirra og veitingu þjónustu
 - Uppfylli kröfur Persónuverndarlaga
 - Uppfylli aðrar kröfur sem sértæk eru fyrir þjónustusvið (t.d. heilbrigðisþjónustu)



Efla samvinnu og samstarf á breiðum vettvangi

- Heilbrigðisþjónusta er mjög mikilvæg sem innviðir í samfélaginu – forsenda lífsgæða og öryggis
- Gögn um heilbrigði eru með viðkvæmustu gögnum borgaranna – ábyrgð er dreifð og skipt
- Viðbrögð við alvarlegum atvikum mikilvægur þáttur í öryggi þjóðarinnar
- Byggir á stafrænum innviðum, traustumhverfi og grunnlagi samskipta og neta
- Nauðsynlegt að efla vitund og auka gallapolni rafrænna lausna – og tryggja skilvirka atvikastjórnun hjá stofnunum og annarri nauðsynlegri þjónustu



Hvernig hækkum við netöryggisstig Íslands?

Embætti landlæknis

- Með samvinnu og samstillingu í þróun og uppbyggingu netöryggis mikilvægra innviða
- ...og við þurfum öll að koma að því – líka þú!



Takk fyrir!

Arnaldur F. Axjörð
Verkefnastjóri öryggismála
arnaldur.axfjord@landlaeknir.is

Miðstöð rafrænna heilbrigðislausna
Embætti landlæknis