Er þjóðfélagið í stakk búið að takast á við netárásir?

Bætt netöryggi innviða
Innleiðing **NIS**-tilskipunarinnar

Hrafnkell V. Gíslason
Vera Sveinbjörnsdóttir

INNANRÍKISRÁÐUNEYTIÐ

PÓST- OG FJARSKIPTASTOFNUN

Netárásir

- Tilgangur árásaraðila
  - Skemmdarverk, fjárhagslegur hagnaður, komast yfir upplýsingar, athygli, völd, ...
- Afleiðingar þolanda
  - Upplýsingaleki, fjárhagstjón, álitshnekkir, truflun, kúgun, óvænt samkeppni, ...
- APT (Advanced Persistent Threat), DDoS (Denial of Services)
- Reynir á viðbúnað vegna raunlægs öryggis (t.d. afritun) sem og vegna netöryggis (t.d. innbrotavarnir – IPS)
- Ekki er að draga úr netárásum
- Alþjóðlegt eðli netárása
  - Samræmd alþjóðleg viðbrögð
- Grafa undan trausti almennings á rafrænum samskiptum

Heildstæð stefnumótun

- Stefnumótun ESB um stafrænan innri markað

  Þrjár megin stoðir og 16 aðgerðir:
  - 1) Bætt aðgengi að vörum og þjónustu á netinu
    - Viðskipti yfir landamæri, geo blocking, höfundaréttur, neytendavernd, vsk í netverslun, póstþjónusta
  - 2) Skapa réttar aðstæður til að stafræn net og þjónustur blómstri
    - Endurskoðun löggjafar, þ.á m. varðandi: Fjarskipti (EECC), fjölmiðlalög, **persónuvernd** á netinu, og netöryggi (**NIS**-tilskipunin)
  - 3) Hámarka vaxtarmöguleika starfræns evrópsks markaðar
    - Stöðlun og samvirkni, e-Government Action Plan, frjálst flæði upplýsinga (skýjaþj.).
- Stefna um net- og upplýsingaöryggi (2015-2026)

  Fjögur meginmarkmið:
  - Efld geta, aukið áfallaþol, bætt löggjöf, traust löggæsla
- Ný fjarskiptaáætlun
- Leiðir af sér fjölmargar lagabreytingar hérlendis

NIS tilskipunin 2016/1148 um öryggi net- og upplýsingakerfa

- Meginmarkmið er að auka hæfni aðildarríkja til að bæta netöryggi og bregðast við aðstæðum þar sem netöryggi er raskað, bæta samvinnu aðildarríkja á sviði netöryggis og styrkja stoðir mikilvægra innviða og nauðsynlegrar þjónustu þar sem netöryggi kemur við sögu
- **Gerðar verða kröfur til rekstraraðila mikilvægra innviða og nauðsynlegrar þjónustu um að sinna tilteknum lágmarksöryggisráðstöfunum og tilkynna öryggisatvik til innlendra yfirvalda**

NIS tilskipunin 2016/1148 um öryggi net- og upplýsingakerfa

Aðildarríkjum ber að:

- Setja sér stefnu um net- og upplýsingaöryggi
  - Skilgreina stefnumótandi markmið, stefnu og reglur um ráðstafanir
  - Gera áhættumat
- Tilnefna tengilið (single point of contact)
- Tilnefna netöryggissveit, CERT/CSIRT sveit
  - Sveitir aðildarríkjanna mynda svo samstarfsnet CSIRT sveita sem skiptast á upplýsingum, samræma viðbrögð o.fl.
- Sjá til þess að þessar stofnanir geti sinnt verkefnum sem tilskipunin kveður á um

Rekstraraðilar mikilvægra innviða og nauðsynlegrar þjónustu

(e. Operators of essential services)

- Hugtakið er skilgreint á eftirfarandi máta:
  1. Þjónustan er nauðsynleg til að viðhalda mikilvægum þjóðfélags eða efnahagslegum verkefnum
  2. Þjónustan byggir á net- og upplýsingakerfum
  3. Atburður gæti haft veruleg og truflandi áhrif á það að þjónustan sé veitt
- Aðildarríkjum ESB ber að skilgreina rekstraraðila nauðsynlegrar þjónustu og uppfæra á a.m.k. 2ja ára fresti

Verulega truflandi áhrif

(e. Significant disruptive effect)

- **Mat á verulega truflandi áhrifum**:
  - Fjöldi notenda sem reiða sig á þjónustu
  - Rekstraraðilar nauðsynlegrar þjónustu háðir þjónustu
  - Áhrif öryggisatvika á efnahaglega og samfélagslega starfsemi og almannaöryggi
  - Markaðshlutdeild
  - Landfræðileg útbreiðsla
  - Mikilvægi til að viðhalda nægilegri þjónustu
    - Hægt að leita annað um sömu þjónustu?
  - Aðildarríki geta þurft að taka tillit til mismunandi aðstæðna í mismunandi geirum við matið.

Til hverra nær tilskipunin – Innviðastarfsemi

Undir hvern heyrir málaflokkurinn + eftirlitsstjórnvald (frumgreining)

- **Orka (rafmagn, olía, gas)**
  - Atvinnuvega- og nýsköpunarráðuneytið, Orkustofnun
- **Flutningar (Loft, vatn/sjór, vegir)**
  - Innanríkisráðuneytið, Samgöngustofa, Vegagerðin
- **Bankar og fjármálainnviðir (Kauphöll, RB, ...)**
  - Fjármála og efnahagsráðuneyti, FME
- **Heilbrigðisgeirinn**
  - Heilbrigðisráðuneytið, Landlæknir
- **Drykkjarvatn (framleiðsla og dreifing)**
  - Umhverfisráðuneytið?, Umhverfisstofnun?, Sveitarfélög?
- **Stafrænir innviðir (IXP, DNS þjónustuveitendur, Top Level Domain skráningaraðilar) ásamt stafrænum þjónustuveitendum**
  - Óljóst

INNANRÍKISRÁÐUNEYTIÐ

PÓST- OG FJARSKIPTASTOFNUN

Meginkröfur um öryggi (14.gr)
(óopinber þýðing)

- **Skilgreindir aðilar þurfa að uppfylla kröfur:**
- Aðildarríki skulu tryggja að rekstraraðilar mikilvægrar þjónustu grípi til **viðeigandi og hæfilegra tæknilegra og skipulagslegra ráðstafana** til að takast á við þá áhættu sem stafar að öryggi net- og upplýsingakerfa sem þeir nota í starfsemi sinni
- Þessar ráðstafanir skulu **tryggja öryggisstig** net- og upplýsingakerfa í samræmi við metna áhættu og nýjustu tækni
- Aðildarríkin skulu tryggja að rekstraraðilar mikilvægrar þjónustu **grípi til viðeigandi aðgerða** til að fyrirbyggja og lágmarka tjón sem hlýst af atvikum tengdum öryggi net- og upplýsingakerfa slíkra rekstraraðila með það að markmiði að tryggja **samfellu** í rekstri slíkra kerfa

Raunlægt- og netöryggi

- Skjalfesta skipulag upplýsingaöryggis með öryggisstefnu
- Framkvæma áhættumat m.t.t. nýjustu krafna
- Skipuleggja og innleiða öryggisráðstafanir á grundvelli áhættumats
- Geta sýnt fram á að þetta ferli sé í samræmi við þær kröfur sem eðlilegt er að þjóðfélagið gerir til þeirra innviða sem vernda skal hverju sinni
- Sambærilegt við 47. grein fjarskiptalaga
- Þarf að huga að e.k. ISO vottun (t.d. ISO 27001)?

Áhættumat þarf að taka mið af netöryggi (cyber security)

- Fjallar oftast um ógnir er stafa af mannavöldum
- Nauðsynlegar tæknilegar og skipulagslegar ráðstafanir til að
  - Gera fyrirfram ráðstafanir til að lágmarka skaða sem hlotist getur af netárás (öryggisflokkun gagna, afritun, dulritun, viðbragðsáætlun, ...)
  - Fyrirbyggja *netárás* (tæknibúnaður, verkferlar og þjálfun starfsfólks)
  - Hafa upplýsingar um stöðu mála hverju sinni
  - Uppgötva og takast á við netárás
  - Tilkynna netárás og bregðast við ábendingum í kjölfarið
- Það er og verður alltaf í verkahring og á ábyrgð rekstraraðila að gera nauðsynlegar ráðstafanir!

Skylda að tilkynna um atvik

- Skylt að tilkynna atvik eins fljótt og auðið er
- Stjórnvöld þurfa að skipuleggja ferlið vel
  - Persónuvernd, CERT-tengiliður, lögreglan, eftirlitsaðili á viðkomandi fagsviði, ...
- Miðlun upplýsinga um netárásina
- Ástandsvitund: Hver er staða mála nú og hvernig er þróun mála?
  - Sams konar árás oft reynd víða

INNANRÍKISRÁÐUNEYTIÐ

PÓST- OG FJARSKIPTASTOFNUN

Hvernig vinnur CERT-ÍS?

- Ráðleggur um ráðstafanir til að fyrirbyggja netárás eða minnka skaða
- Tekur við tilkynningum um atvik
- Ástandsvitund um almenna stöðu / heildaryfirsýn
- Aðstoðar við að meðhöndla atvik í samráði við þolanda
  - Almenn greiningarhæfni á tæknilegum þáttum netárása
- Sem landstengiliður: sendir og tekur við upplýsingum um netógnir frá erlendum aðilum
- Miðlar upplýsingum
  - Milli aðila
  - Frá upplýsingaveitum til aðila
  - Sérhæfð þjálfun
- Skipuleggur og framkvæmir æfingar
- Cert-ÍS er landstengiliður, megináhersla á fjarskipti. Getur gert samninga
  - Grein 47. í fjarskiptalögum
- Unnið að gerð samnings vegna stjórnarráðsins (Gov-CERT)

Innleiðingarferill

- Innanríkisráðuneyti fer með málaflokkinn netöryggi, en þörf er á víðtæku samráði og/eða samstarfi við fleiri ráðuneyti og stofnanir
  - **Fjölmargir hagsmunaaðilar** – víðtækt samráð
  - Getum við nýtt okkur netöryggisráð?
  - Samráðsvettvangur með hagsmunaaðilum?
- Hlutverk PFS / CERT-ÍS?
- Hlutverk annarra eftirlitsstjórnvalda?

Innleiðingarferill - Drög að tímalínu

Janúar 2017	Vinnuhópur settur á laggirnar
Febrúar 2017	Greiningarvinna hefst
Mars 2017	Opið samráð hefst
Maí 2017	Vinnuhópur lýkur störfum
Maí-Sept 2017	Drög að frumvarpi
Okt-Nóv 2017	Opið samráð um frumvarp
Nóv-Des 2017	Lokagerð frumvarps
Vor 2018	Afgreiðsla frumvarps á þingi

Erum við í stakk búin að takast á við netárás?

- Meginmarkmið NIS tilskipunarinnar er að auka hæfni aðildarríkja til að bæta netöryggi og bregðast við aðstæðum þar sem netöryggi er raskað
  - **Lágmarksviðmið** til **afmarkaðs** hóps
  - Aðildarríki geta útvíkkað nálgunina (fleiri aðilar)
- Efla samræmingu og samtal milli aðila
- Er þetta nóg?
  - Þarf að endurskoða **högun** upplýsingakerfa ríkisins?

Takk fyrir!

Spurningar?