Fjarskiptastofa

Netöryggislöggjöf og innlit í NIS-2

Unnur Kristín Sveinbjarnardóttir, sviðsstjóri stafræns öryggis
unnur@fjarskiptastofa.is
18. október 2023

Efni kynningar

1. Skilaboð Evrópu
2. Netöryggislög nr. 78/2019
3. Innlit í NIS-2
4. Staða innleiðingar


Digital Compass for Europe
Skills
Foster citizens' digital skills and train more ICT specialists
Public services
Digitalise public services and medical records
Infrastructure
Gigabit connections for all households
Business


DIGITAL DECADE
POLICY PROGRAMME
2030 | THE WAY FORWARD


NIS Directive


CYBERSECURITY
CERTIFICATION
ON CLOUD SERVICES


INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK
Promoting Interoperability among EU Risk Management Frameworks
ENISA REPORTS
enisa


Introducing the upcoming CYBER RESILIENCE ACT.


enisa
EU CYBERSECURITY
ENTERS INTO FOR
A new era for ENISA
and cybersecurity


NIS2
DIRECTIV


5G
THREAT
LANDSCAPE
enisa


Digital sovereignty
What does this mean for the EU, and how can it be achieved?


New EU
Cybersecu
Strategy


Cybersecurity of 5G networks
EU Toolbox of risk mitigating measures
CG Publication
01/2020
NIS COOPERATION GROUP

“You can´t have a high level of cybersecurity if you don´t have a minimum level of cybersecurity.”

Juhan Lepassaar, Executive Director - ENISA

Fjarskiptastofa

Netöryggislög

Netöryggislög *- markmið*

Fjarskiptastofa

Lög nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða tóku gildi 1. september 2020.

- Byggja á NIS-1 tilskipun ESB frá árinu 2016.
- Hefur það markmið *að bæta net- og upplýsingaöryggi rekstraraðila á mismunandi sviðum atvinnulífsins sem veita samfélagi okkar og atvinnulífi nauðsynlega þjónustu.*
- Í þessu felst tvíhliða nálgun:
  - Innleiða fyrirbyggjandi ráðstafanir um áhættustýringu og viðbúnað til að koma í veg fyrir atvik eða takmarka tjón af atvikum *(kröfur+eftirlit).*
  - Skilvirkt viðbragð við áhættu og atvikum og ástandsvitund *(netöryggissveit).*
- Ýmis sérlög kveða á um öryggi og virkni þjónustu, svo sem á sviði fjarskipta, samgangna, fjármálaþjónustu, á sviði traustþjónustna o.fl.

Netöryggislög *- gildissvið*

Fjarskiptastofa

- NIS-lögin gilda um mikilvæga innviði sem greinast í tvo flokka:
  1. *Rekstraraðila nauðsynlegrar þjónustu (RNÞ) á eftirfarandi þjónustusviðum, að uppfylltum skilyrðum,:*
     - bankastarfsemi og innviða fjármálamarkaða, flutninga, heilbrigðisþjónustu, orku-, hita- og vatnsveitna, svo og stafrænna grunnvirkja.
     - - þjónusta er nauðsynleg fyrir viðhald mikilvægrar samfélagslegrar og efnahagslegrar starfsemi (sjá II. kafla reglug. 866/2020),
       - veiting þjónustu er háð net- og upplýsingakerfum og
       - atvik hefðu verulega skerðandi áhrif á veitingu þjónustu.
  2. *Veitendur stafrænnar þjónustu á sviði netmarkaðar, leitarvélar á netinu og skýjavinnsluþjónustu.*
- Eftirlitsstjórnvöld tilnefna RNÞ til ráðherra sem birtir skrá í B-hluta Stjórnartíðinda.
- Í dag eru 53 aðilar skilgreindir sem RNÞ. (uppfærsla væntanleg)
- Ekki þarf tilnefningu fyrir veitendur stafrænnar þjónustu. (örfélög og stærri)

- Gilda um net- og upplýsingakerfi sem eru undirstaða fyrir veitingu þjónustu.

Netöryggislög *- lágmarkskröfur*

Fjarskiptastofa

- Settar eru lágmarkskröfur um áhættustýringu og viðbúnað, felst efnislega í að:
  - skjalfesta stefnu og ferla til að meta, stýra og lágmarka áhættu sem steðjað getur að öryggi net- og upplýsingakerfa þeirra,
  - setja sér öryggisstefnu, framkvæma áhættumat reglubundið og ákvarða og endurmeta öryggisráðstafanir á grundvelli þess,
  - hafa skjalfesta viðbragðsáætlun og áætlun um samfelldan og órofinn rekstur og þjónustu til að tryggja takmörkun á tjóni ef alvarleg röskun verður á starfsemi þeirra.
  - **tilkynna** um alvarlega áhættu og atvik til CERT-ÍS sem miðlar til eftirlitsstjórnvalda.
- Nokkuð ítarleg heimild til ráðherra til að setja reglugerðir.
- Aðili skal byggja á gildandi alþjóðlega viðurkenndum stöðlum um bestu framkvæmd á sviði net- og upplýsingaöryggis:
  - ISO/IEC 27001, 27002, 27005 og aðra sértæka staðla og reglur á hlutaðeigandi sviði.
- Þetta þýðir í raun krafa um að **innleiða, viðhalda og bæta stöðugt stjórnunarkerfi upplýsingaöryggis** viðkomandi aðila.

Reglugerðir nr. 866/2020 og 1255/2020

Reglugerðir *– stjórnunarkerfi upplýsingaöryggis*

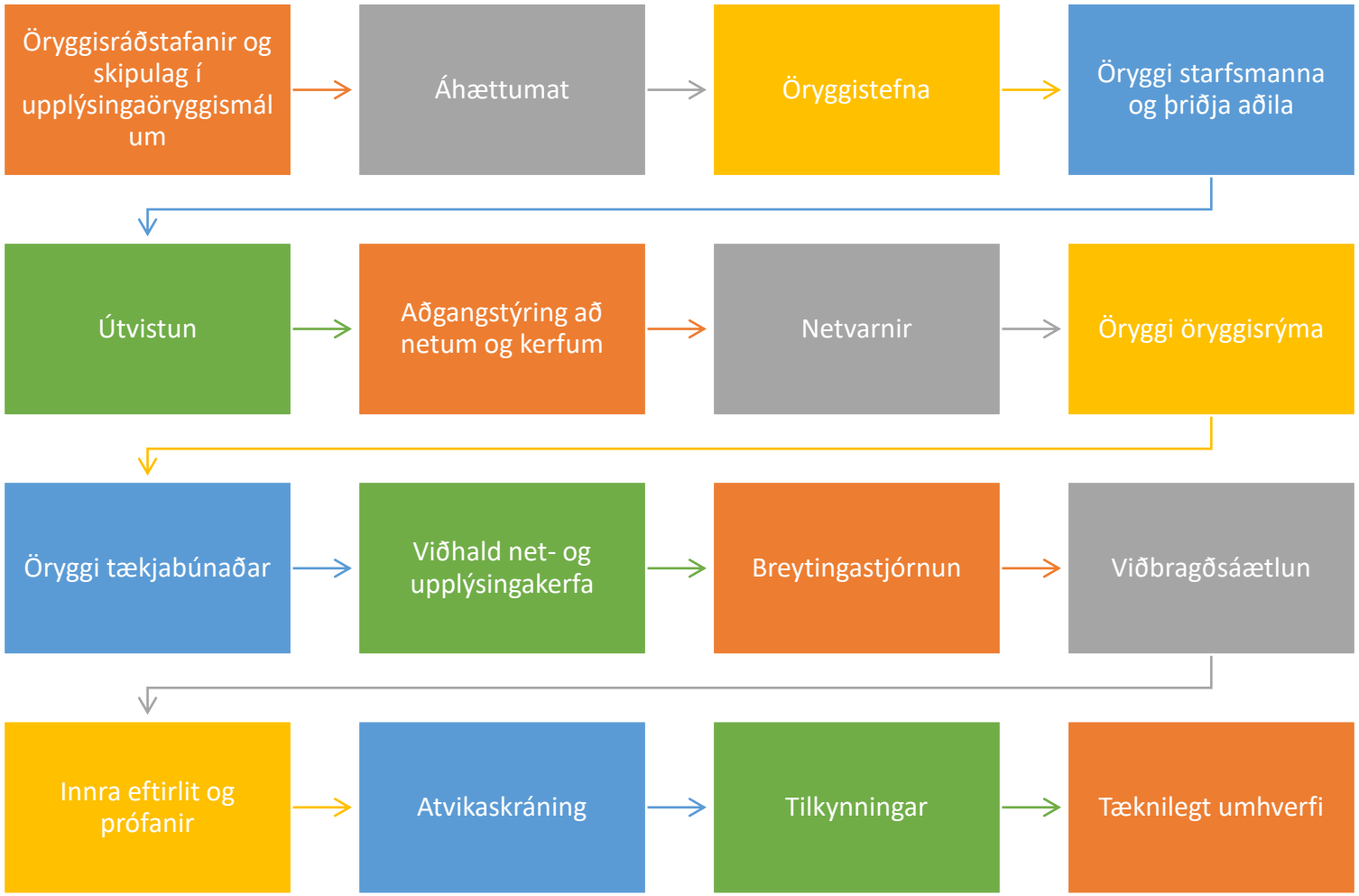
Fjarskiptastofa

Hvað er stjórnkerfi upplýsingaöryggis (ISMS)

- Þetta er kerfisbundin og heildstæð nálgun til tryggja með sem bestum hætti að **leynd, réttleiki eða tiltækileiki** upplýsinga glatist ekki.
- Þetta felur í sér að fyrirtæki grípi til viðeigandi og hlutfallslegra tæknilegra (technical) og skipulagslegra (organizational) ráðstafana til að stjórna, á viðeigandi hátt, áhættu sem steðjar að öryggi neta og þjónustu.

Þetta er hringrásarverkefni sem hefur ekki endapunkt!

Reglugerðir *– stjórnunarkerfi upplýsingaöryggis*



Netöryggislög *- eftirlitsstjórnvöld*

Fjarskiptastofa

- Eftirlitsstjórnvöld á grundvelli laganna eru:
  - Embætti landlæknis
  - Orkustofnun
  - Samgöngustofa
  - Seðlabanki Íslands (FME)
  - Umhverfisstofnun
  - Fjarskiptastofa – samhæfingarstjórnvald
- Stjórnvöldum er heimilt að gera úttektir og prófanir á því hvort rekstraraðilar nauðsynlegrar þjónustu uppfylli kröfur netöryggislaga og reglugerða sem settar eru á grundvelli þeirra.
- Ber að gefa út bindandi fyrirmæli til aðila ef frávik er á hlítni við lágmarkskröfur laganna.
- Hafa heimildir til álagningu dagsekta og stjórnvaldssekta.

Fjarskiptastofa

NIS-2 tilskipun

Af hverju NIS-2?

Ekki öll mikilvæg starfsemi innan gildissviðs	Ósamræmi í gildissviði milli aðildarríkja (RNÞ)	Mismunandi lágmarkskröfur netöryggis milli aðildarríkja
Mismunandi þröskuldar fyrir atvikatilkynningar	Ómarkvisst og takmarkað eftirlit	Ekki skyldubundin miðlun upplýsinga milli aðildarríkja og milli aðila

Stoðir NIS-2

GETA AÐILDARRÍKJA	SKYLDUR Á AÐILA	SAMSTARF OG UPPLÝSINGAGJÖF
Eftirlitsstjórnvöld	Ábyrgð æðstu stjórnenda	NIS samstarfshópur
CSIRTs	Stjórnkerfi net- og upplýsingaöryggis (lágmarkskröfur)	CSIRTs samstarf
Netöryggisstefnur	Tilkynningarskylda	CyCLONe
Upplýsingagjöf um veikleika		Gagnagrunnur um veikleika
Rammi um hættustjórn		Skýrslugjöf ENISA

Gildissvið NIS-2 *- sektorar*

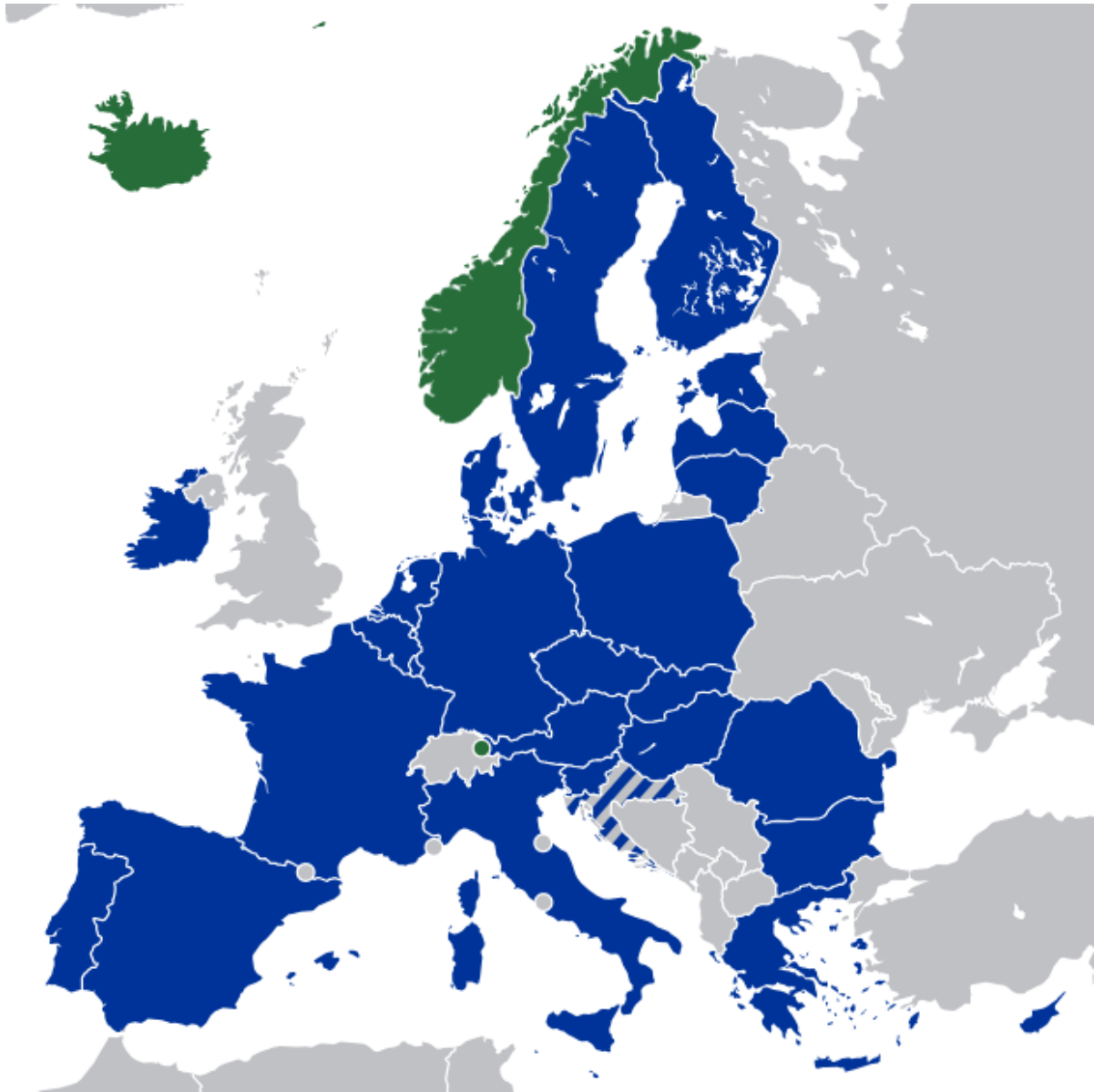
Viðauki I - Nauðsynleg þjónusta	**Viðauki II** - Mikilvæg þjónusta
Orka (rafmagn, svæðisbundin hitun, olía, gas og vetni)	Póst- og sendingarþjónusta
Samgöngur (loft, vatn vegir, lestir)	Úrgangsstjórnun
Bankastarfsemi (DORA)	Efni/Lyf (framleiðsla og dreifing)
Innviðir fjármálamarkaða (DORA)	Matvæli (framleiðsla, vinnsla og dreifing)
Heilbrigði (heilbr.þjónusta, rannsóknir og framleiðsla lyfja og lækningatækja)	Framleiðsla (lækningatæki, tölvur, fjarskiptavörur, rafmagnsvörur, vélar, bílar og flutningstæki)
Drykkjarvatn	Veitendur stafrænnar þjónustu (leitarvélar á netinu, netmarkaðir og "social networks")
Úrgangsvatn	Rannsóknir
Stafræn grunnvirki (IXP, DNS, TDL, skýjaþjónustur, gagnaver, dreifinet efnis, fjarskiptafyrirtæki, traustþjónustur)	
"ICT Service Management"	***Rautt = nýtt í NIS-2**
Geimur	
Opinberar stofnanir	

NIS-2 tilskipun *- gildissvið*

Fjarskiptastofa

Almenna reglan um hverjir falla undir NIS-2

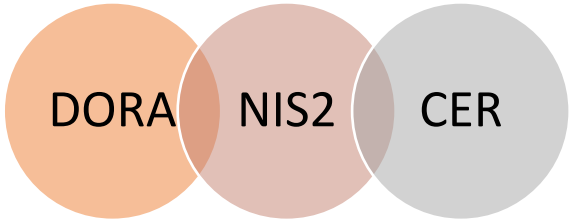
- Veita þjónustu sem tilgreindar eru í viðauka I eða II við tilskipunina.
- Eru meðalstór eða stór fyrirtæki í skilningi Evrópuréttar.
- Veita þjónustu innan evrópska efnahagssvæðisins.
- Einkaaðilar og opinberar stofnanir.



NIS-2 tilskipun *- gildissvið*

Aðilar sem falla undir NIS-2, óháð stærð:

- Fjarskiptafyrirtæki.
- Traustþjónustuveitendur.
- Skráningarstofur höfuðléna (TLD) og þjónustuveitendur lénsheitakerfa (DNS).
- Opinberar stofnanir.
- Aðilar sem eru einu veitendur þjónustu á tilteknu sviði.
- Aðilar sem veita “krítíska” þjónustu þar sem truflanir á henni geta haft áhrif á almannahag eða kerfisleg áhrif (CER).
- Aðilar sem þegar eru skilgreindir rekstraraðilar nauðsynlegrar þjónustu. (valkvætt)



NIS-2 *- Samræmdar lágmarkskröfur*

Fjarskiptastofa

Ábyrgð æðstu stjórnenda

- Æðstu stjórnendur skulu staðfesta stjórnskipulag netöryggis, hafa yfirsýn yfir innleiðingu þess og bera ábyrgð á skorti á hlítingu.
- Æðstu stjórnendur skulu hljóta þjálfun og hafa þekkingu og getu til að meta áhættuþætti og stjórnskipulag netöryggis í fyrirtæki sínu.

Stjórnskipan netöryggis

- Áhættumiðuð nálgun.
- „All-hazards“ nálgun.
- Lágmarkskröfur settar fram í tilskipun.
- Afram kröfur um stjórnskipan netöryggis.

NIS-2 *- Samræmdar lágmarkskröfur*

Aðilar þurfa að:

Innleiða viðeigandi tæknilegar, rekstrarlegar og stjórnskipulegar ráðstafanir til að stýra áhættu.

Koma í veg fyrir eða lágmarka áhrif atvika á viðskiptavini sína og aðra þjónustu.

Nær til net- og upplýsingakerfa sem að aðili notar fyrir rekstur sinn eða veitingu þjónustu sinnar.

NIS-2 – tilgreindar lágmarkskröfur

Fjarskiptastofa

Til viðbótar við almennt stjórnskipulag eru lágmarkskröfur um:

- Stefnur um áhættumat og net- og upplýsingakerfi.
- Atvikameðhöndlun.
- Rekstrarsamfellu, endurreisnaráætlun og hættustjórn.
- Öryggi net- og upplýsingakerfa m.t.t. innleiðingu kerfa, þróun og viðhalda, þ.m.t. veikleikagreiningu og upplýsingagjöf.
- Öryggi birgjakeðju, þ.m.t. öryggistengda þætti sem varða tengsl við birgja og þjónustuveitendur.
- Stefnur og ferla til að meta virkni stjórnskipulags og öryggisráðstafana.
- Lágmarksaðferðir hvað varðar þjálfun.
- Stefnur varðandi dulkóðun.
- Öryggisráðstafanir varðandi starfsfólk, aðgangsstýringar og fleira.
- Notkun fjölþátta auðkenningarleiða, örugg tal-, mynd- og textasamskipti og örugg neyðarsamskipti innan fyrirtækis.
- Tilkynningarskylda um alvarleg atvik.

Aðildarríki þurfa að taka sérstakt tillit til birgjakeðju ICT í netöryggisstefnum sínum.

NIS-2 - *eftirlit*

Það eru ítarleg ákvæði um eftirlit í NIS-2:

- Rík krafa um áhættumiðað eftirlit.
- Sett er mun ítarlegri ákvæði um framkvæmd eftirlits t.a.m.:
  - Framkvæmd úttekta
  - Öryggisprófana
  - Rannsókn atvika
  - Kröfu um tímasettar úrbætur
  - Álagningu sekta sem og afturköllun starfsleyfam (nauðsynleg)
  - Perónuleg ábyrgð stjórnenda
  - O.fl.

- Áfram gerður greinarmunur á eftirliti milli nauðsynlegra aðila (ex-ante + ex-post) og mikilvægra aðila (ex-post).

Innleiðing NIS-2 tilskipunar

Staða á NIS-1

- Innleidd í EES-samninginn í febrúar 2023. Var ekki skyldubundin fyrir EFTA-ríki en þó tekin upp í EES-samninginn.
- Ísland (2019) og Liechtenstein (2023) hafa innleitt í landsrétt. Noregur hefur ekki innleitt NIS-1 (frumvarp komið).

Staðan á NIS-2

- Tilskipunin er EES-tæk (ólíkt NIS-1).
- EFTA skrifstofa í Brussel og vinnuhópar þar vinna að innleiðingu.
- Óvíst hvenær innleiðingardagsetning verður m.t.t. ESS/EFTA ríkja.
- Ráðuneyti háskóla, iðnaðar og nýsköpunar fer með forræði á innleiðingu tilskipunarinnar hér á landi.
  - Er á aðgerðaráætlun fyrir netöryggisstefnu stjórnvalda.
- Ljóst er að mikil greiningarvinna og samvinna við aðila þarf að eiga sér stað við innleiðingu.

Fjarskiptastofa