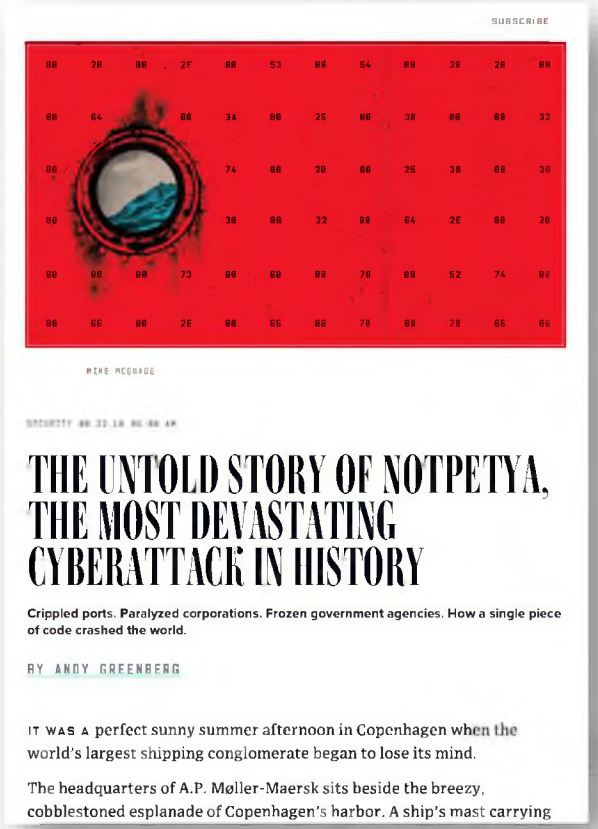
Frumvarp til laga um netöryggi

Innleiðing NIS-tilskipunarinnar á Íslandi
Kynning fyrir umhverfis- og samgöngunefnd Alþingis
21/3 2019

Gagnagíslataka nú í vikunni: Norsk Hydro

```
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts
everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:
```



SUBSCRIBE

MIKE MCGRATH

SECURITY 08.22.18 06:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

BY ANDY GREENBERG

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

The headquarters of A.P. Møller-Maersk sits beside the breezy, cobblestoned esplanade of Copenhagen's harbor. A ship's mast carrying

Tjón **danska skipafélagsins Maersk** vegna **NotPetya** er metinn á um **200 – 300 milljóna USD (24 – 36 milljarða ISK)**

Tjón annarra alþjóðlegra fyrirtækja er metið **enn meira** (Merck, FedEx og Saint-Gobain).

Tjón **Mondelez** og **Reckitt Benckiser** var einnig verulegt.

theregister.co.uk

Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it's 'an act of war'

Snack company client disagrees, sues for $100m

By Kieren McCarthy in San Francisco 11 Jan 2019 at 00:19 48 SHARE ▼

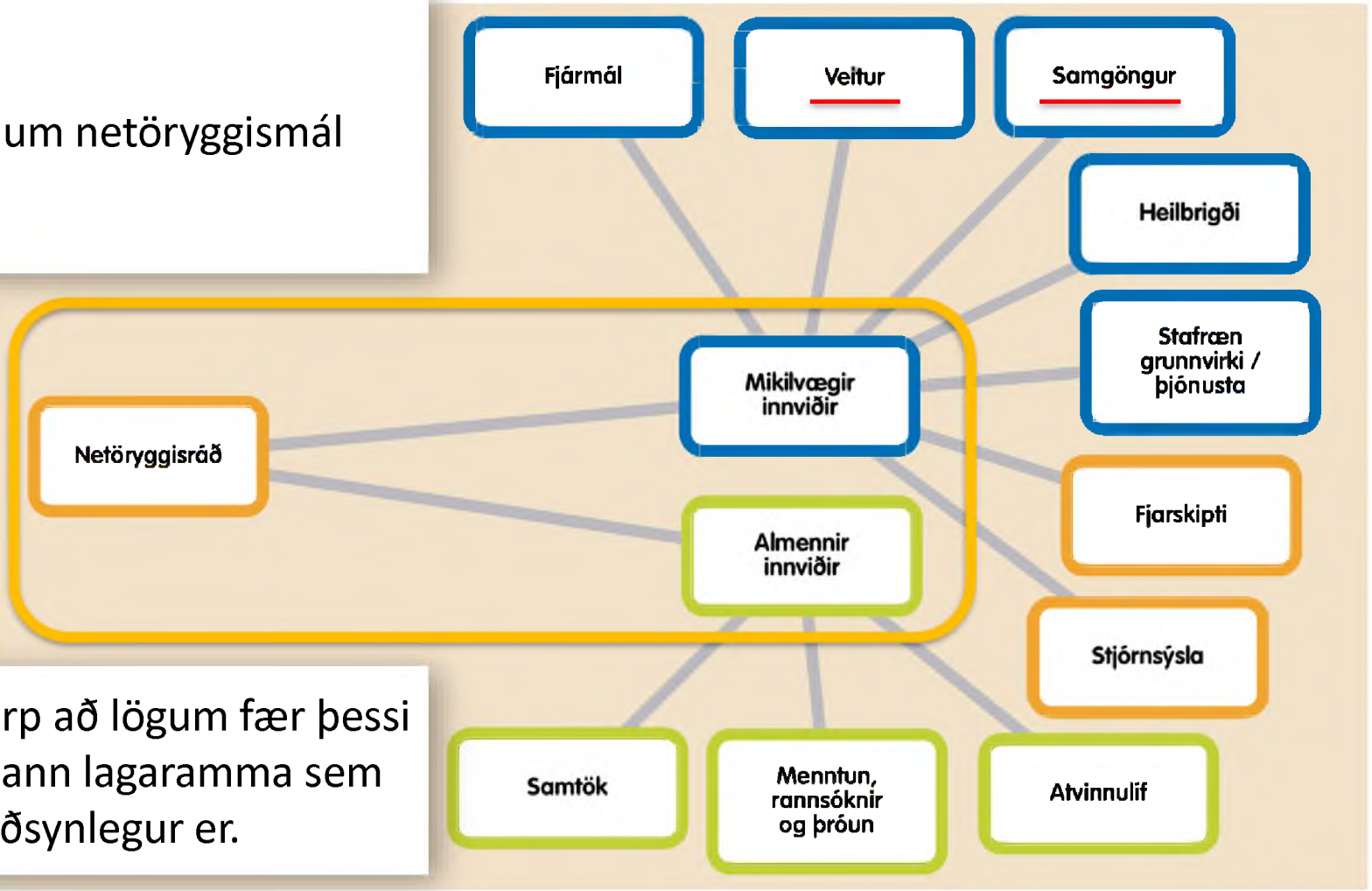
(Grein úr WIRED, ágúst 2018)

Ör þróun innan Evrópu: Að skapa sameiginlegan ramma um netöryggi þjónustu og tækni, NIS-tilskipunin markar bara byrjun

Ný netöryggisstefna Evrópusambandsins

- Kynnt sem tillaga 13. september 2017, **samþykkt 10. des. 2018**.
- **Efla evrópsku netöryggisstofnunina, ENISA** og gefa henni aukið vægi, en þó að settum ákveðnum skorðum þannig að réttindi og skyldur aðildaríkja séu ekki skert.
- Mótun **vottunarkerfis netöryggis fyrir nettæki og þjónustu** (e. *European Cybersecurity Certification Schemes*, *ECCS, for Information and Communication Technology, ICT, products and services*).
  - Með þessu er ekki stefnt að þróun nýrra staðla, heldur frekar að aukinni og samræmdri notkun þeirra staðla sem fyrir eru til að unnt sé að skapa skilvirkara markaðssvæði innan Evrópu.

Samstarf um netöryggismál



Verði frumvarp að lögum fær þessi samvinna þann lagaramma sem nauðsynlegur er.

Meginmarkmið frumvarpsins og nýmæli

- ✓ Að samræma lágmarkskröfur um áhættustýringu og viðbúnað mikilvægra innviða
- ✓ Að innleiða tilkynningaskyldu um alvarleg atvik
- ✓ Að gera stjórnvöldum betur kleift að samræma viðbrögð við netógnum
- ✓ Að efla og útvíkka starfsemi netöryggissveitar

Þskj. 557 – 416. mál

- ❖ Fyrsti heildstæði lagabálkurinn um netöryggi á Íslandi?
- ❖ Virk stefnumótun og eftirfylgni af hálfu stjórnvalda
- ❖ Netöryggisráð

Stuðla að því að **koma í veg fyrir rof á nauðsynlegri þjónustu** í samfélaginu

Frumvarp til laga um öryggi net- og upplýsingakerfa mikilvægra innviða

- Undirbúningur fyrir innleiðingu hér á landi hófst vorið 2017
- NISD á lista ríkisstjórnar yfir forgangsmál vegna hagsmunagæslu Íslands gagnvart ESB (2016-17 og 2018)
- Samráð við önnur ráðuneyti, stofnanir, hagsmunaaðila og almenning
- Drög að frumvarpi voru birt í samráðsgátt stjórnvalda í júní 2018
- Frumvarp til nýrra heildarlaga, auk breytinga á gildandi lögum um fjarskipti og Póst- og fjarskiptastofnun (PFS)
- Frávik frá NISD: Tillaga er um að fella hitaveitur undir mikilvæga innviði svo og netöryggis-þjónustu við Stjórnarráðið

Hverjir munu falla undir nýja löggjöf?

6. gr. óðskýr.

MIKILVÆGIR INNVIÐIR

Opinberar stofnanir
Fjarskiptafyrirtæki

Rekstraraðilar nauðsynlegrar þjónustu

Bankar/innviðir, flutninga-starfsemi, heilbrigðis-þjónusta, veitur, stafræn grunnvirki

Veitendur stafrænnar þjónustu

Netmarkaðir, leitarvélar á netinu, skýjavinnsluþjónusta

Eftirlitsstjórnvöld

NETÖRYGGI

Eftirlitsstjórnvöld (11. gr.)

- **Fjármálaeftirlitið** vegna bankastarfsemi og tiltekinna innviða
- **Samgöngustofa** vegna flutningastarfsemi
- **Landlæknir** vegna heilbrigðisþjónustu
- **Orkustofnun** vegna hita- og orkuveitna
- **Umhverfisstofnun** vegna vatnsveitna
- **Póst- og fjarskiptastofnun** vegna stafrænna grunnvirkja og *stafrænna þjónustuveitenda*

- Stöðugt og markvisst aðhald mikilvægt
- Eftirlitsheimildir (12. gr.)
- Tengsl við önnur lög (5. gr.)

PFS jafnframt ætlað að stuðla að samræmdri framkvæmd fyrirhugaðra laga (***samhæfingarstjórnvald**, 13. gr.*)

MIKILVÆGIR INNVIÐIR

Áhættustýring og viðbúnaður (7. gr.)

- *Lágmarkskröfur* (sérlög, ef við á)
- Skjalfest stefna og ferlar til að meta, stýra og lágmarka áhættu
- Reglubundið áhættumat og endurmat öryggisráðstafana
  - Tæknilegar og skipulagslegar ráðstafanir
  - Horfa til viðurkenndra viðmiða um bestu framkvæmd
- Áætlun um viðbúnað og samfelldan rekstur
  - Lágmarka mögulegt tjón, tryggja viðeigandi viðbrögð við atvikum
  - Atvikagreining
- Virkt innra eftirlit

MIKILVÆGIR INNVIÐIR

Tilkynningaskylda (8. gr.)

- Mikilvægir innviðir skulu **án tafar** tilkynna netöryggissveit PFS um alvarleg atvik/áhættu sem ógnar öryggi kerfa þeirra
  - Atvik sem hafa, eða ástæða er til að ætla að geti haft, veruleg áhrif á net- og upplýsingaöryggi í starfsemi hlutaðeigandi
  - Skylda til að upplýsa um útvistunarfyrirkomulag, ef við á, og hugsanleg smitáhrif, jafnvel yfir landamæri (netöryggissveit miðlar upplýsingum til tengiliða erlendis, ef við á)
  - Upplýsingar um atvik aðgengilegar eftirlitsstjórnvöldum án tafar – Vefgátt í þróun
- Netöryggissveit: Landsbundið öryggis- og viðbragðsteymi
  - Sólarhringsvöktun > sveitin ráðgefandi um viðbrögð/aðgerðir
  - Samstarf við ríkislögreglustjóra, ef við á

Aðgangur að upplýsingum (17. gr.)

- Vegna viðbragða við atvikum skal heimila aðgang að upplýsingum og gögnum sem netöryggissveit metur nauðsynleg, eins skjótt og við verður komið
  - Tryggja þarf sveitinni bestu faglegu forsendur til viðbragða
  - Eftir atvikum samráð við eftirlitsstjórnvöld
- Skjalfestar vinnureglur um öflun upplýsinga, viðeigandi ráðstafanir til að tryggja öryggi og eyðingu gagna, friðhelgi einkalífs og öryggis- og viðskiptahagsmuni
  - Sjá og heimild til vinnslu persónuupplýsinga skv. 21. gr.

Þjónusta netöryggissveitar (14., 16., 27. gr.)

- Greining, snemmviðvaranir, upplýsingamiðlun
- Mótar stöðumynd vegna netógna á hverjum tíma, eftir því sem við á
  - Reglubundin miðlun til netöryggisráðs, í samræmi við óskir þess
- Sólarhringsvöktun vegna atvikatilkynninga
  - Samstarf við ríkislögreglustjóra, ef við á
- Aðstoð og leiðbeiningar um sérhæfðar forvarnir í tengslum við öryggi net- og upplýsingakerfa
  - Mikilvægir innviðir, Stjórnarráð Íslands, aðrar opinberar stofnanir og fjarskiptafyrirtæki
- Tæknileg vöktunarþjónusta í boði
  - Mikilvægir innviðir, opinberar stofnanir og fjarskiptafyrirtæki
  - Ábyrgð eiganda/rekstraraðila verður þó ekki útvistað

Samstarf og miðlun (10., 18., 27. gr.)

- Skipulegt samstarf, á viðeigandi forsendum
  - Samráðs- og sviðshópar
  - Viðbúnaðaræfingar

- Miðlun tilkynninga til almennings um veikleika og almennar hættur, í samráði við lögreglu og eftirlitsstjórnvöld
- Umfjöllun um stöðu og þróun net- og upplýsingaöryggismála í árlegri skýrslu PFS

Þagnarskylda (19.-20. gr.)

- Starfslið eftirlitsstjórnvalda, samhæfingarstjórnvalds, netöryggissveitar og netöryggisráðs er bundið sérstakri þagnarskyldu
- Þó er þeim heimilt að miðla gögnum/upplýsingum sín í milli og gagnvart lögreglu- og persónuverndaryfirvöldum, ef þær varða framkvæmd netöryggislaga, almannavarnir eða persónuvernd
  - Einnig gagnvart erlendum aðilum, s.s. vegna alþjóðasamvinnu á sviði netöryggis
  - Trúnaðar skal gætt um öryggis- og viðskiptahagsmuni
  - Varnarmálalög, ef við á

Nánari upplýsingar

Ítarefni og tenglar	www.stjr.is/netoryggi www.stjornarradid.is/netoryggi