Hvernig stuðla CERT-IS og stafrænt öryggi að bættu netöryggi?

Bjarki Þór Sigvarðsson, fagstjóri hjá CERT-IS
Sigrún Lilja Sigmarsdóttir, fagstjóri hjá stafrænu öryggi

Stafrænt öryggi

Sigrún Lilja Sigmarsdóttir – fagstjóri eftirlits með öryggi net- og upplýsingakerfa

Fjarskiptastofa

Lögreglan á höfuðborgarsvæðinu
6dagar ·

Netsvik: Nýtt form á smishing árásum

Atlagan miðar að því að yfirtaka heimabanka með alv

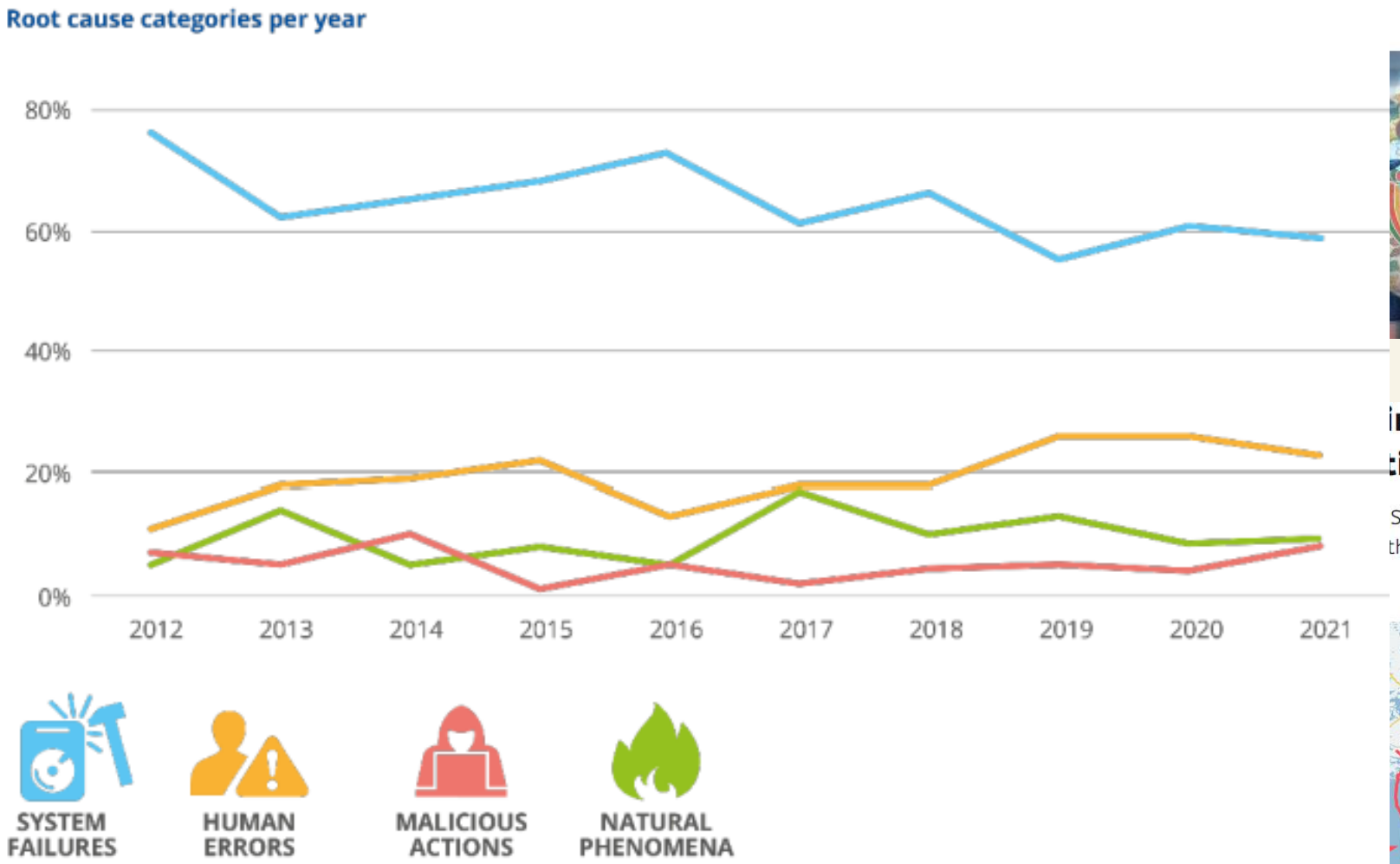
Smishing er form vefveiða þar sem glæpamenn send
Þetta hefur verið algegnt form netárása á Íslandi og
kominn til móttakanda og tengill á síðu þar sem þarf
gjald en þessar upplýsingar eru síðan notaðar til að

MO - Smishing árás til yf

Hraunið komið yfir

Óttar Kolbeinsson Proppé skrifar · 21. maí 2021 18:01

Figure 3: Root cause categories for telecom security incidents in the EU reported over 2012-2021 period



Netsvik margfaldast á þremur árum: Hvað ber að varast?

stórir tilboðsdagar á netinu fara að bresta
prósent síðustu þrjú ár.

A A A

ing to help with
tion

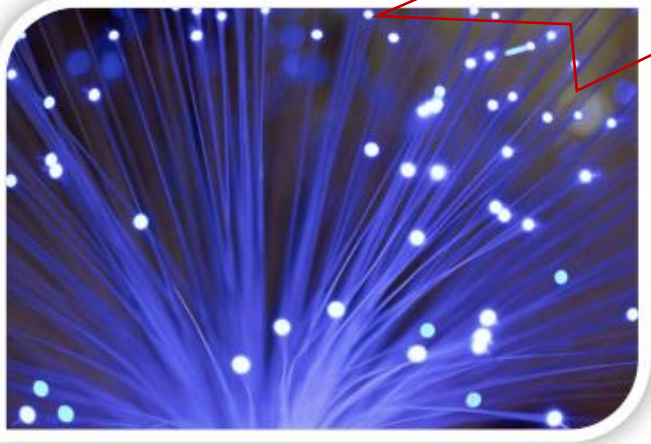
Secretary General Jens Stoltenberg
the investigations," the president

PFS(20)-05

Fjarskipti

Stefna Póst- og fjarskiptastofnunar

um öryggi og virkni fjarskiptainnviða



Póst- og fjarskiptastofnun
MARS 2020

NIS

STEFNA FJARSKIPTASTOFU

UM FYRIRKOMULAG OG FRAMKVÆMD EFTIRLITS
MEÐ REKSTRARAÐILUM STAFRÆNNA GRUNNVIRKJA

OKTÓBER 2021

Í endurskoðun

Fjarskiptastofa

NIS

Stefna Fjarskiptastofu

- Að eftirlit Fjarskiptastofu stuðli að auknu öryggi og viðnámsþrótti upplýsinga- og netkerfa rekstraraðila stafrænna grunnvirkja
- Að hafa eftirlit með því að rekstraraðilar stafrænna grunnvirki hlíti NIS-löggjöfinni og afleiddri reglugerð
- Að hafa yfirsýn yfir stöðu öryggis net- og upplýsingakerfa rekstraraðila stafrænna grunnvirkja

Fjarskiptastofa

Verkfærakista eftirlits

- **Áhættumiðað eftirlit:**
  - Þekkingaröflun – **Sjálfsmat fyrirtækja**
  - Úttektir
  - Tæknilegar prófanir, t.d. penetration tests
  - Rannsókn atvika *(ex-post)*

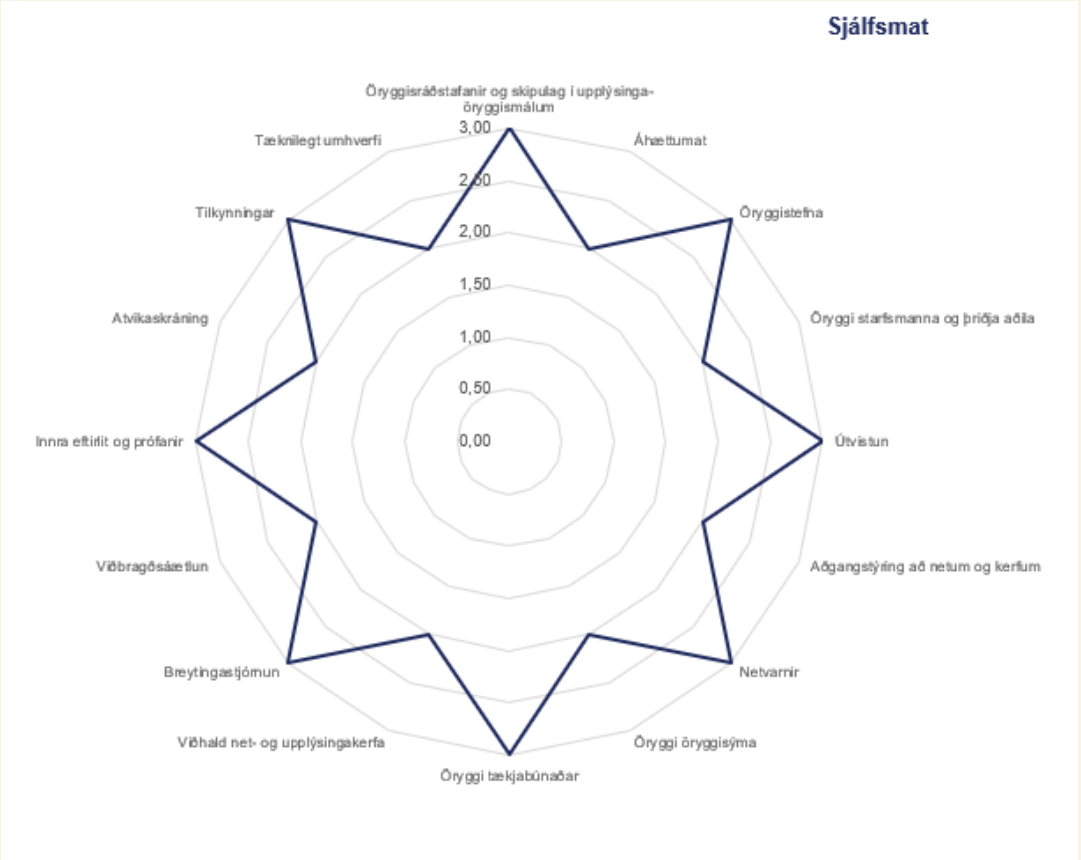
- Heildstætt áhættumat á mikilvægum fjarskiptainnviðum og kerfum
- Sérstakt áhættumat, kerfisþáttum eða ógnum

Ástandsvitund

Fjarskiptastofa

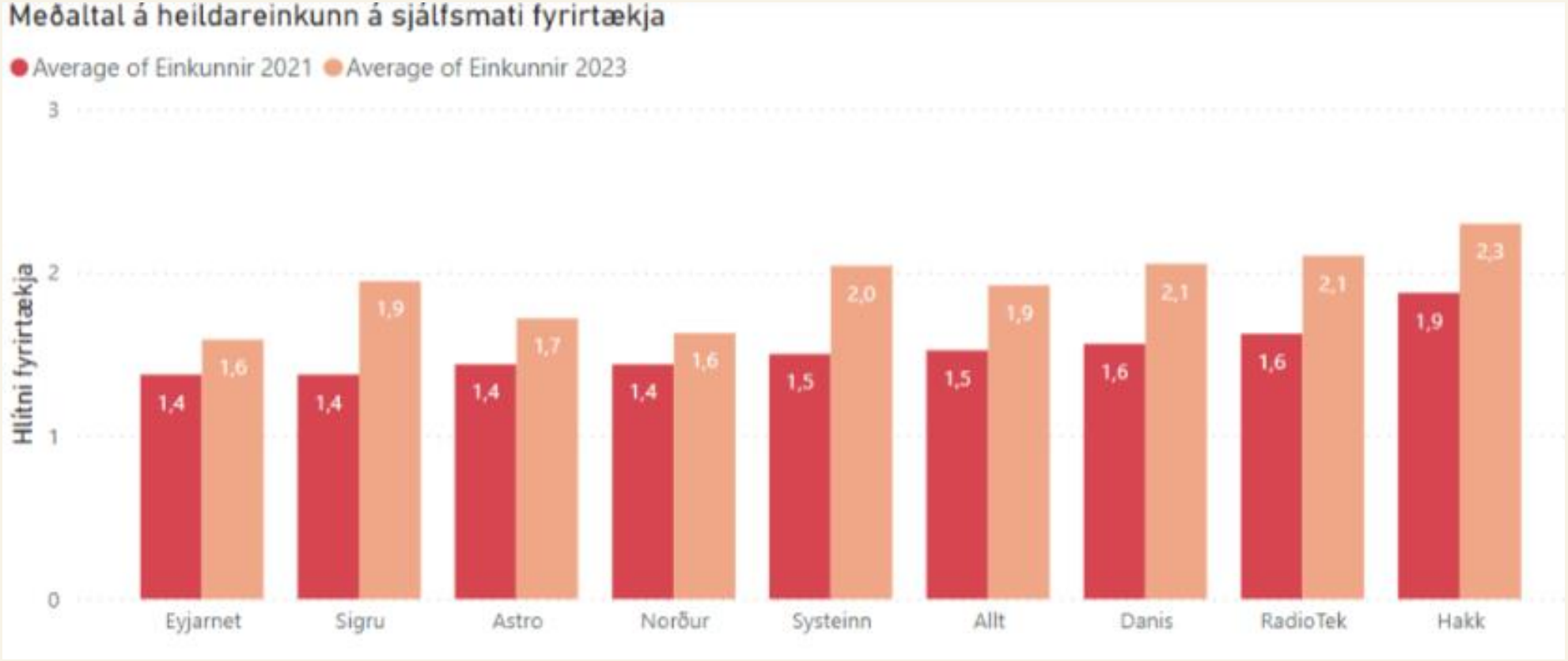
Sjálfmat fyrirtækja

- Sjálfsmat fyrirtækja gefur mikilvægar upplýsingar um almenna stöðu öryggismála hjá viðkomandi félögum sem og heildstæðari sýn yfir markaðinn
- Að lokinni yfirferð Fjarskiptastofu er samantekt niðurstaðna sjálfsmatsins send til hvers fyrirtækisins
- Sjálfsmötin eru grundvöllur afmörkunar og forgangsröðunar frekara eftirlits



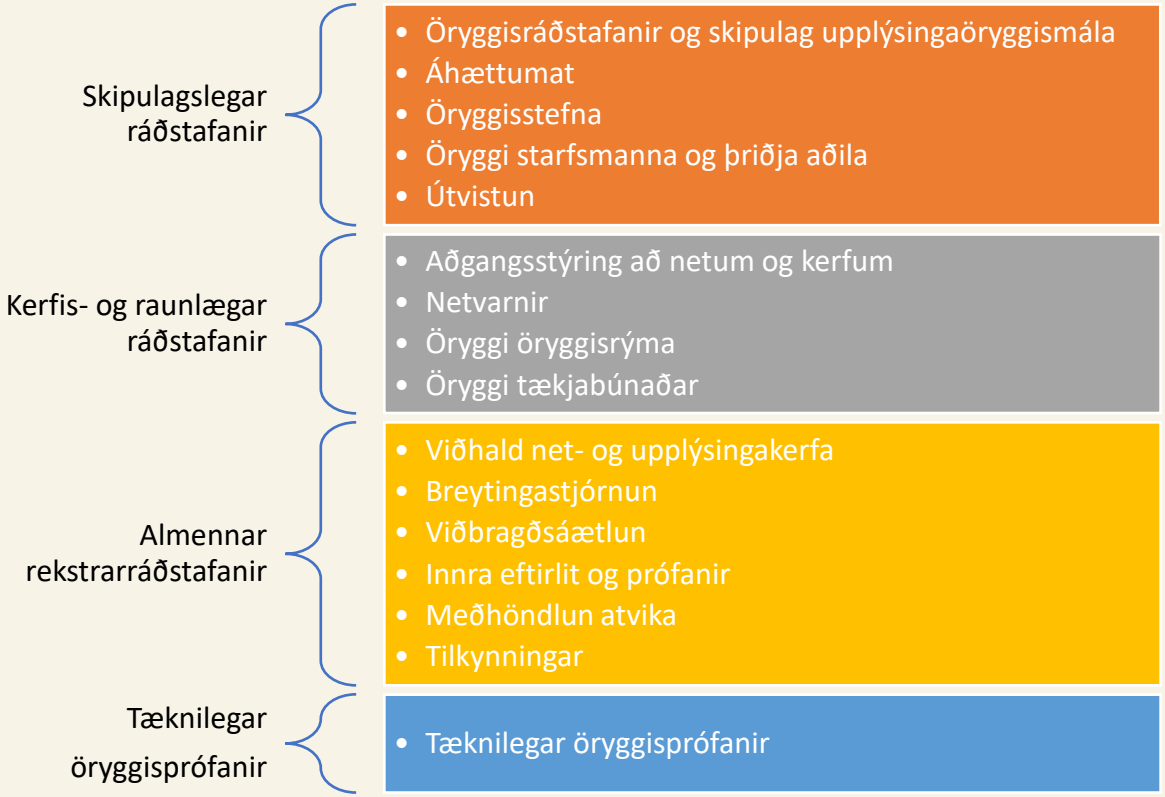
Fjarskiptastofa

Sjálfsmat – Yfirsýn yfir stöðu fyrirtækja



Fjarskiptastofa

Úttektir



Niðurstöður	
Kafli	**Mat á stöðu**
Skipulagslegar ráðstafanir	**0,90**
Öryggisráðstafanir og skipulag upplýsingaöryggismála	0,00
Áhættumat	1,10
Öryggisstefna	3,00
Öryggi starfsmanna og þriðja aðila	0,00
Útvistun	2,00

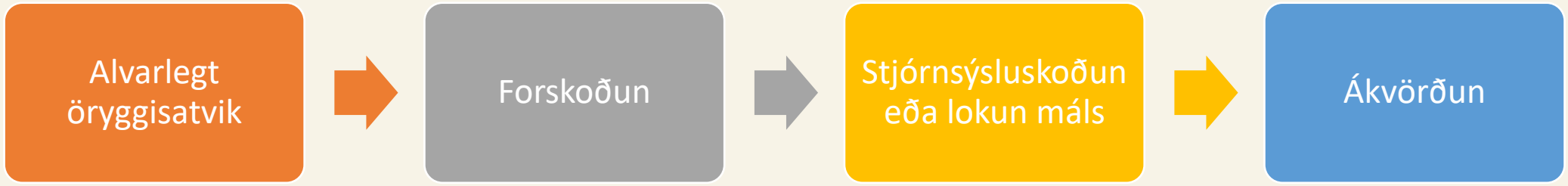
Fjarskiptastofa

Tæknilegar öryggisprófanir

- Prófun á kerfislægum öryggisráðstöfunum fyrirtækis
- Ytri aðili framkvæmdir innri og/eða ytri innbrotsprófun
- Prófunin veitir upplýsingar um veikleika hjá fyrirtækjum
- Prófunin gefur mikilvægar upplýsingar um virkni öryggisráðstafana hjá viðkomandi félögum sem og heildstæðari sýn yfir markaðinn

Fjarskiptastofa

Stjórnsýsluskoðanir á alvarlegum öryggisatvikum



Fjarskiptastofa

Áhættumöt

- Almennt áhættumat
  - Áhættumat ógna sem geta valdið alvarlegum truflunum á virkni fjarskiptaneta og/eða rofi á veitingu fjarskiptaþjónustu, annað hvort á stórum landssvæðum, og/eða hvort áhrifin vörðuðu mikinn fjölda notenda
- Sértækt áhættumat
  - í sértækum áhættumötum er kallað eftir að fyrirtæki endurmeti ákveðnar ógnir út frá viðurkenndri aðferðafræði sem og leggja mat á öryggisráðstafanir sínar út frá niðurstöðu slíks mats

Fjarskiptastofa

Ávinningur

- Sjálfsmöt
- Úttektir
- Tæknilegar prófanir
- Rannsókn atvika
- Áhættumöt

Umbætur fyrirtækja

Aukið netöryggi

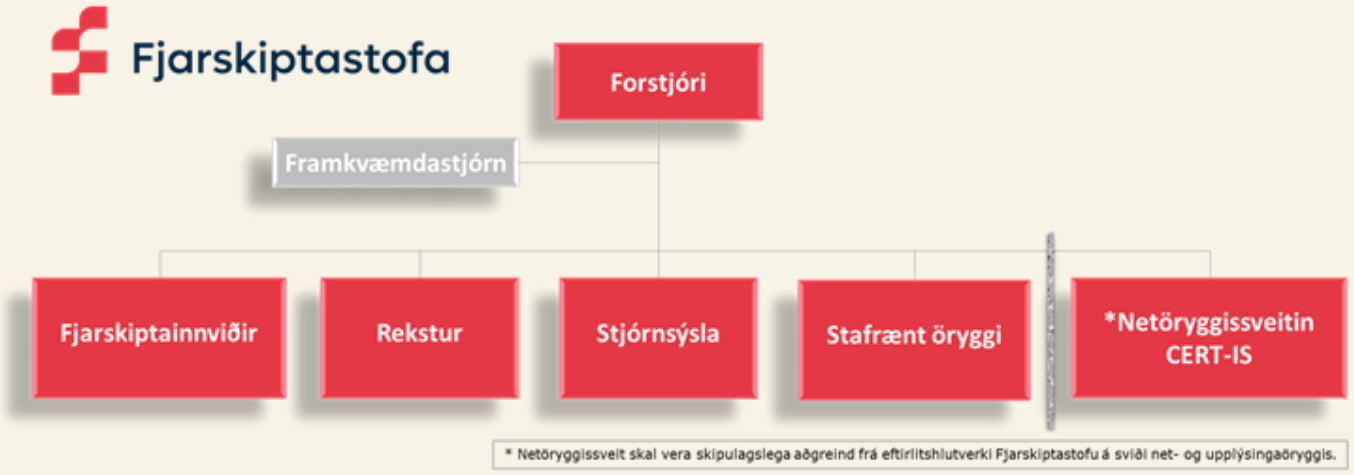
Fjarskiptastofa

CERT·IS

Bjarki Þór Sigvarðsson - Fagsjóri ástandsvitundar

CERT-IS

- *CERT-IS gegnir hlutverki landsbundins öryggis- og viðbragðsteymis vegna ógna, atvika og áhættu er varðar net- og upplýsingaöryggi (þjóðar-CSIRT)*
- Sjálfstæð eining undir Fjarskiptastofu
- Atvikameðhöndlun & Ástandsvitund



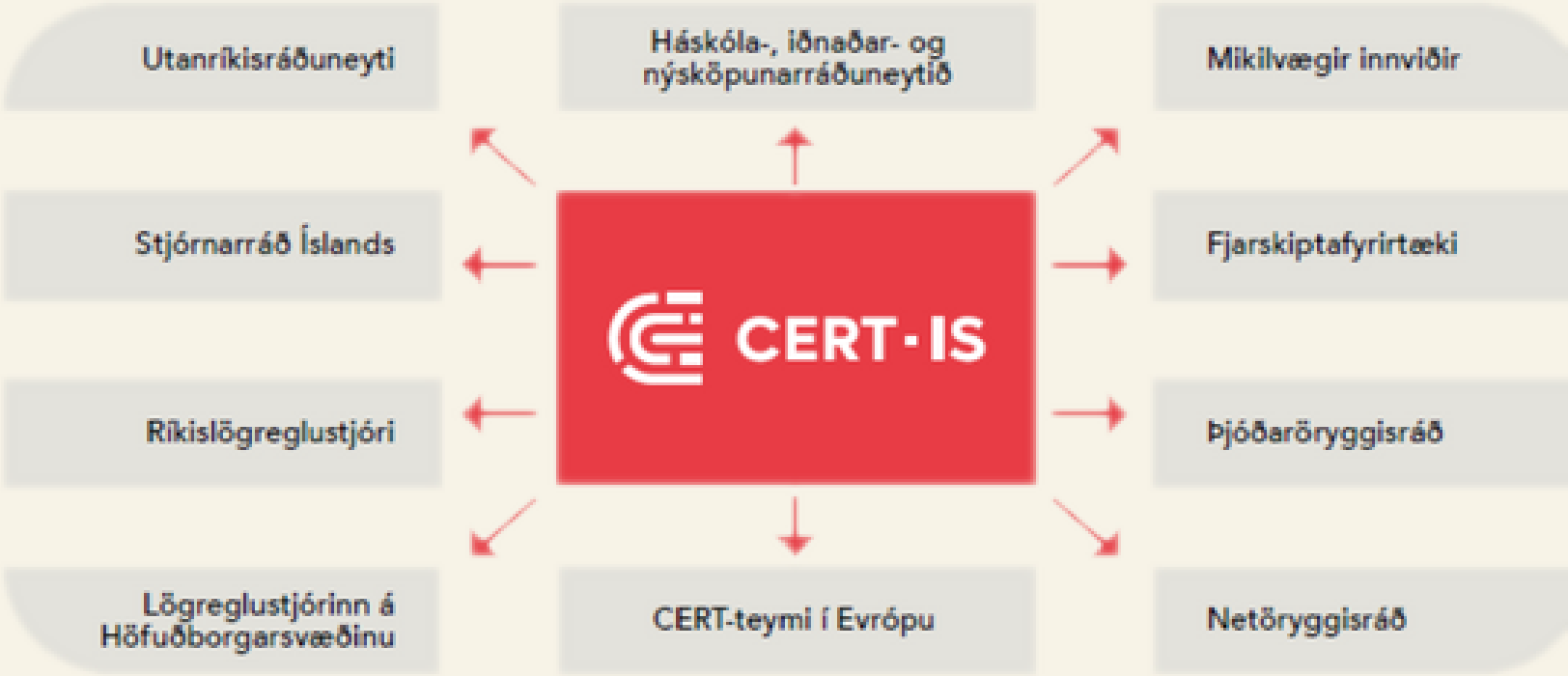
CERT·IS

Hlutverk CERT-IS

- Fyrirbyggja og draga úr hættu á netárásum
- Styðja við skjót viðbrögð
- Stuðla að viðeigandi ástandsvitund í netöryggismálum
- Stuðla að markvissum og samhæfðum viðbrögðum við ógnum, áhættu og atvikum

CERT·IS

Hlutverk CERT-IS



Sviðshópar CERT-IS

- Sviðshópur Fjarskiptainnviða
- Sviðshópur Fjármálainnviða
- Sviðshópur Orkuinnviða
- Sviðshópur Flutningsinnviða
- Sviðshópur Heilbrigðisinnviða

CERT·IS

Verkefni

- Atvikameðhöndlun
- Ógnargreining
- Veikleikagreining og skönnun
- Tæknileg vöktunarþjónusta
  - GOV-CERT
- Fræðsla
  - Ráðstefnur
  - Námskeið
  - Vinnustofur
- Innlent og erlent samstarf
  - Sviðshópar
  - NCC
  - NATO
- Æfingar
  - Locked Shields 2023 - 🥇
  - CISA – Nordic
  - Cyber Coalition

CERT·IS

Ástandsvitund og stöðumynd

7. gr.

Ástandsvitund og stöðumynd vegna netógna.

Netöryggissveitin skal leitast við að skapa viðeigandi almenna ástandsvitund um ógnir, áhættu og atvik innan netumdæmis Íslands.

Netöryggissveit mótar stöðumynd vegna netógna og skal að minnsta kosti árlega skjalfesta og miðla slíku stöðumati til netöryggisráðs. Þá skal netöryggissveit leitast við að upplýsa eftirlitsstjórnvöld reglulega um stöðumynd vegna netógna, eftir atvikum að því er tiltekna þjónustuhópa varðar.

Á grundvelli almennrar ástandsvitundar og stöðumynda vegna netógna á hverjum tíma forgangsraðar og skipuleggur netöryggissveit fyrirbyggjandi aðgerðir og samstarf við og innan þjónustuhópa sveitarinnar, og eftir atvikum, netumdæmis Íslands, í því skyni að sporna við áhættu og atvikum sem ógna öryggi net- og upplýsingakerfa.

CERT·IS

Ástandsvitund og stöðumynd

7. gr.

Ástandsvitund og stöðumynd vegna netógna.

Netöryggissveitin skal leitast við að skapa viðeigandi almenna ástandsvitund um ógnir, áhættu og atvik innan netumdæmis Íslands.

Netöryggissveit mótar stöðumynd vegna netógna og skal að minnsta kosti árlega skjalfesta og miðla slíku stöðumati til netöryggisráðs. Þá skal netöryggissveit leitast við að upplýsa eftirlitsstjórnvöld reglulega um stöðumynd vegna netógna, eftir atvikum að því er tiltekna þjónustuhópa varðar.

Á grundvelli almennrar ástandsvitundar og stöðumynda vegna netógna á hverjum tíma forgangsraðar og skipuleggur netöryggissveit fyrirbyggjandi aðgerðir og samstarf við og innan þjónustuhópa sveitarinnar, og eftir atvikum, netumdæmis Íslands, í því skyni að sporna við áhættu og atvikum sem ógna öryggi net- og upplýsingakerfa.

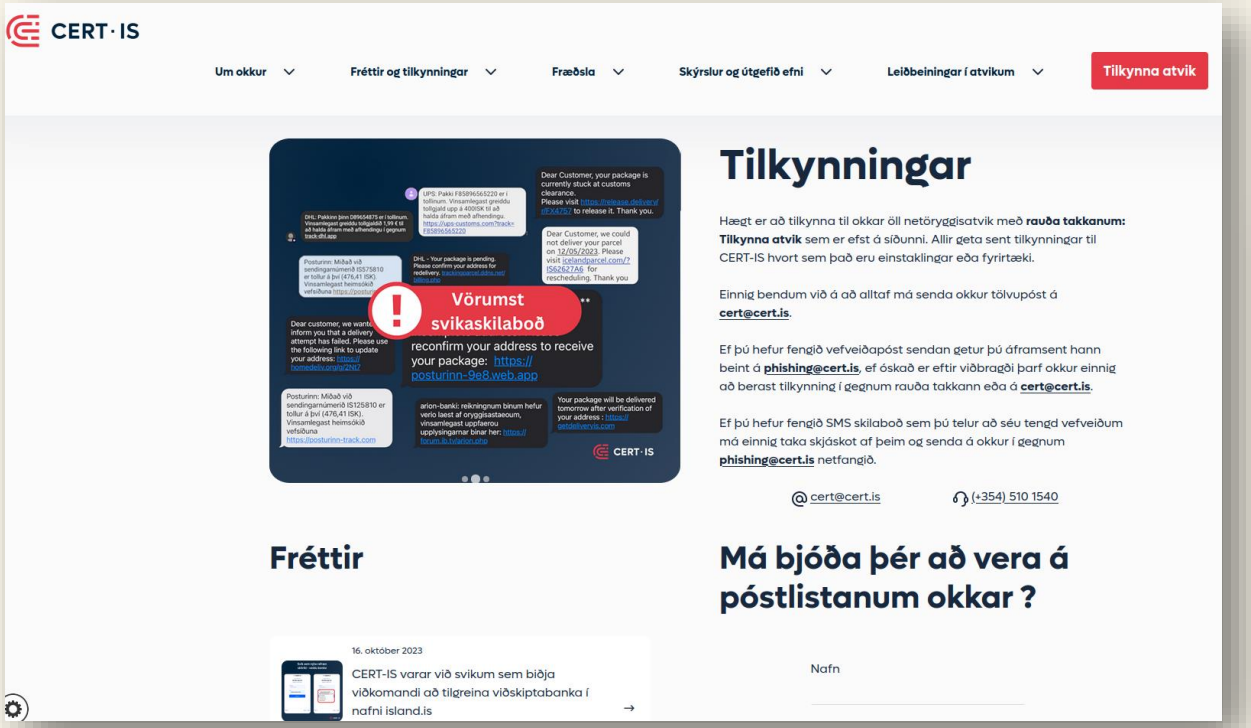
CERT·IS

Tilkynningar frá CERT-IS

- Fáum upplýsingar úr ýmsum áttum
  - Veikleikar
  - Virkni ógnarhópa
  - Atvik
- Miðlun upplýsinga
  - Hver er markhópurinn hverju sinni?
  - Hvernig er besti miðillinn fyrir tilkynningarnar?

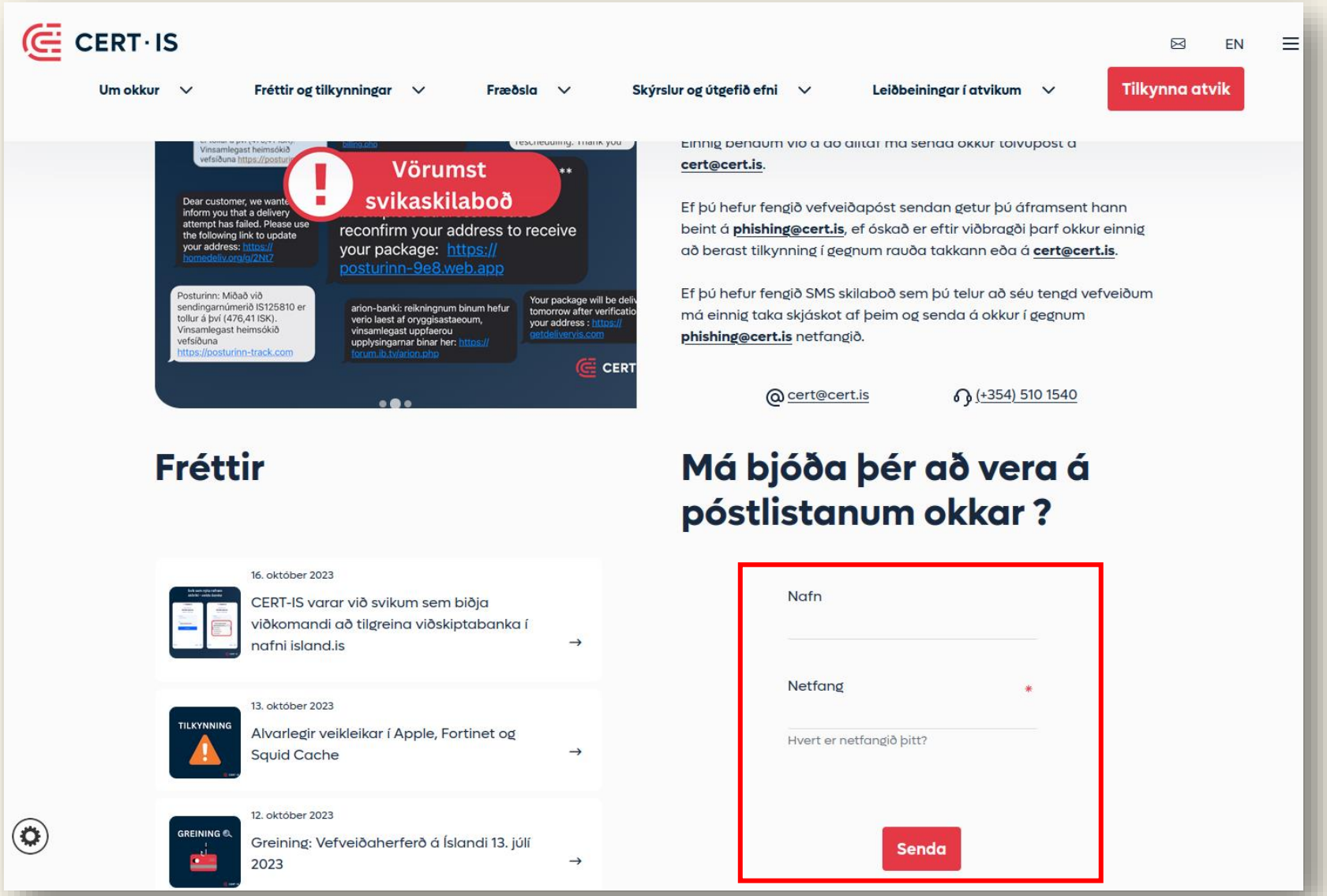
CERT·IS

Almennar tilkynningar



CERT·IS

Veikleikatilkynningar - Póstlisti



CERT·IS

Veikleikatilkynningar - Póstlisti

CERT·IS

Veikleikar í GNU C safninu (glibc), Android og TorchServe

Tilkynnt var um alvarlega veikleika í GNU C safninu, TorchServe og Android. **CERT-IS mælir með að uppfæra án tafa og fylgja leiðbeiningum framleiðanda.**
Vegna veikleikans í Libwebp sem tilkynnt var um gær hafa margir brugðist við og gefið út uppfærslu, Microsoft gaf út uppfærslu fyrir Edge, Teams og Skype [1]. Libwebp er notað í mörgum forritum og vöfrum og mælir CERT-IS með að fólk uppfæri forrit og vafra um leið og uppfærsla hefur verið gefin út.

Veikleiki í GNU C (glibc)

Veikleikinn CVE-2023-4911 með CVSSv3 veikleikastig upp á 7.8 gerir ógnaraðila kleift að öðlast kerfisstjóraréttindi (e. Root privileges) með því að nota veilubragð á yfirflæði í biðminni (e. exploiting a buffer overflow) [2].

Veikleikinn hefur verið uppfærður í glibc 2.34. Fyrir þá sem hafa ekki tök á því að uppfæra í nýjustu útgáfur geta útfært mótvægisaðgerðir [3].

Veikleikar í TorchServe

CERT·IS

Alvarlegur veikleiki í Cisco IOS XE

Cisco hefur tilkynnt um alvarlegan veikleika í Cisco IOS XE web UI [1]. Ekki er til staðar uppfærsla sem lokar á veikleikann. Cisco hefur gefið út leiðbeiningar um hvernig megi koma í veg fyrir misnotkun og skoða hvort misnotkun hafi átt sér stað út frá uppgefnum vísum. **CERT-IS mælir með að fylgja leiðbeiningum framleiðanda eins fljótt og auðið er og fylgjast með frekari tilkynningum frá framleiðanda. Einnig að skoða þá vísa sem koma fram í leiðbeiningum Cisco til að meta hvort veikleikinn hafi verið misnotaður.**
Cisco hefur upplýst um að veikleikinn sé þegar misnotaður af ógnaraðilum.

Alvarlegir veikleikar (e. critical)

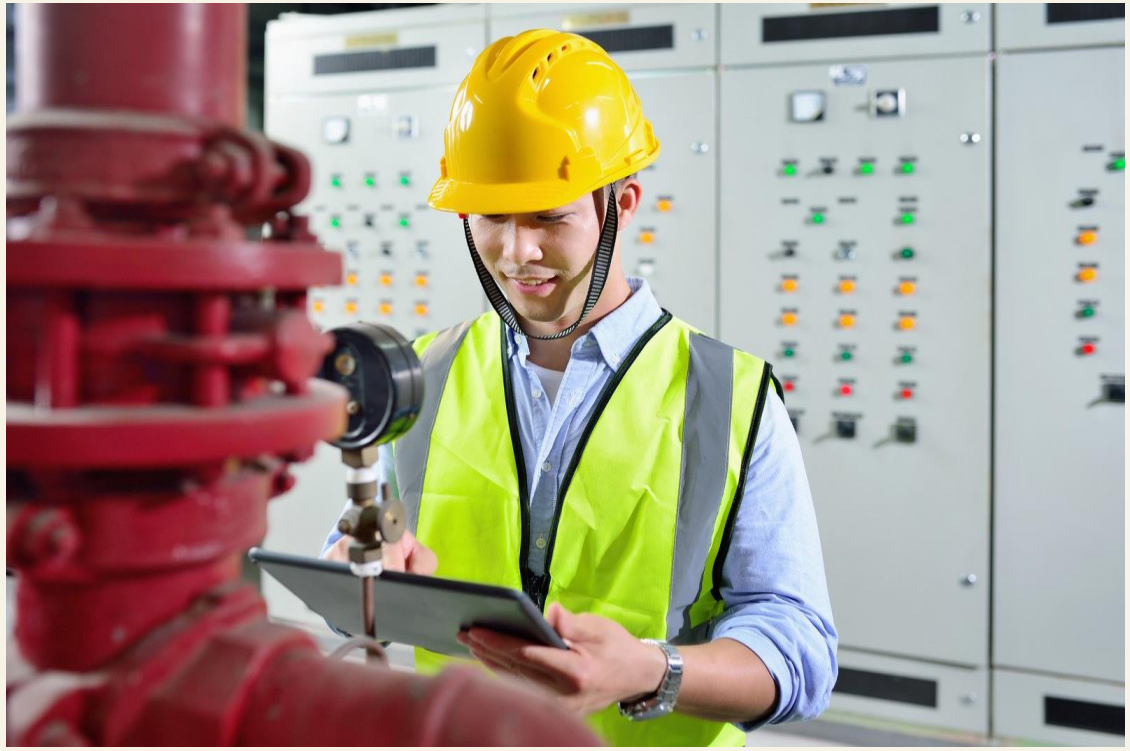
CVE-2023-20198
Veikleikinn CVE-2023-20198 er með CVSS einkunn 10.0 samkvæmt Cisco. Veikleikinn gerir óauðkenndum ógnaraðila kleift að búa til notanda á búnaðinum með mikil réttindi (e. privilege level 15 access) og ná þar með stjórn á búnaðinum.

Leiðbeiningar Cisco

Ráðleggingar Cisco
Cisco mælir með að slökkva á vefaðgengi (e. web UI) að búnaðinum [1] og tekur fram að allur aðgangur að stjórnkerfum (e. management services) þar með talið vefaðgangur (e. web UI) ætti ekki að vera aðgengilegt á netkerfum sem er ekki treyst (e. untrusted networks). Cisco mælir með að vista nýjar stillingar á þann hátt að endurræsing á

CERT·IS

Veikleikatilkynningar - Sviðshópar



Á döfinni

- NIS2 mun margfalda þjónustuhópinn
- Enn frekari stækkun teymisins
- Meiri sjálfvirknivæðing
- Bætt greiningarhæfni
  - Full nýting á tækjum og tólum sem við höfum aðgang að
  - Aukinn sýnileiki á umfang ógnarhópa og veikleika á Íslandi
- Auka sýnileika CERT-IS enn meira
  - *Við sjáum bara það sem við sjáum*

CERT·IS

Allar spurningar eða athugasemdir má senda á

sigrunlilja@fjarskiptastofa.is

bjarki@cert.is