CERT·IS

# Ársyfirlit 2022

CERT-IS er deild innan Fjarrskiptaskofu.
Málefni netöryggis heyra undir háskóla-,
iðnaðar- og nýsköpunarráðuneyti (HVIN)

CERT·IS

# Efni

CERT·IS

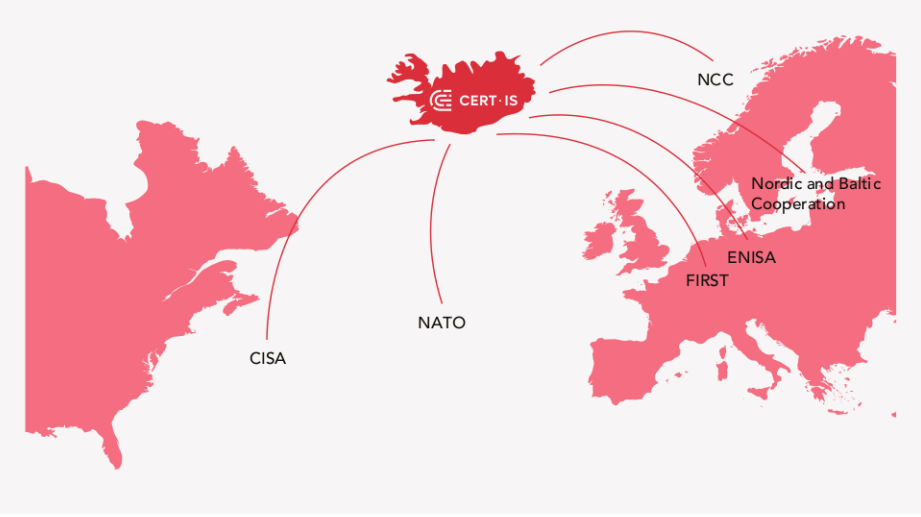
# Ávarp sviðsstjóra

Ársins 2022 verður minnst sem ár mikilla umbrota. Íbúar Evrópu vöknuðu upp við vondan draum þann 24. febrúar við þau tíðindi að allsherjar innrás Rússa í Úkraínu væri hafin. Þrátt fyrir að margir hafi átt erfitt með að trúa nýjum raunveruleika hafði innrásin þó átt sér dágóðan aðdraganda. Vestrænar leyniþjónustur deildu opinskátt upplýsingum með úkraínskum stjórnvöldum og fleirum um að innrás Rússa væri yfirvofandi í aðdraganda innrásarinnar. Einnig má segja að innrás Rússa, og hópum þeim hliðhollum hafi byrjað fyrr með hnitmiðuðum netárásum á Úkraínska innviði þar sem markmiðið virtist fyrst og fremst að valda sem mestum skemmdum.

Nýr veruleiki blasti við hinum vestræna heimi og viðbrögð létu ekki á sér standa. Í kjölfarið hófu aðildarlönd NATO og annarra þjóða að fordæma innrásina og beita Rússland efnahagsþvingunum af áður óþekktum skala, Ísland þar á meðal. Rússnesk yfirvöld brugðust við og tóku skýrt fram að þau lönd er tækju þátt í þvingunum teldust til óvinveittra ríkja og mættu búast við afleiðingum. Fyrir Ísland þýddi það að meta þurfti áhættur íslenskra innviða upp á nýtt. Það sem áður þótti fjarlægur veruleiki var nú allt í einu orðin að raunverulegri ógn og áhættu.

Þessi nýi veruleiki hafði áhrif á áætlanir Netöryggissveitinnar CERT-IS. Sveitin hefur fylgt þriggja ára áætlun um uppbyggingu sem snertir á stöðugildum, innleiðingu búnaðar og þekkingaröflunar sem mun hámarka getu sveitarinnar, í ljósi aðfanga, til að styðja við bakið á íslenskum innviðum og íslenskri stjórnsýslu. Tilefni var til að endurskoða þær áætlanir og flýta uppbyggingu enn frekar til að ná skilgreindum markmiðum fyrr en áætlað hafi verið. Með stuðningi ráðuneytis háskóla, iðnaðar og nýsköpunar náðist að flýta innleiðingu sviðshópa allra mikilvægra innviða. Sviðshóparnir hafa það markmið að tryggja samhæfingu tengdra aðila þegar kemur að viðbrögðum og upplýsinga-gjöf um veikleika, árásir og aðrar ógnir er steðja að þeim ásamt því að framkvæma sameiginlegar netöryggisæfingar. Virkjun sviðshópanna var eitt mikilvægasta verkefni CERT-IS árið 2022.

Með fjölgun starfsmanna CERT-IS undanfarin tvö ár hefur sveitin náð ákveðinni breidd varðandi málaflokkinn. Nú er tímabært að fara á dýptina. Næstu markmið snúa að því að efla greiningargetu sveitarinnar með innleiðingu á réttum tólum og auknu samstarfi við erlendar systurstofnanir. Með mikilvægum og góðum stuðningi stjórnvalda hefur verið hægt að innleiða tól og kerfi sem gefa CERT-IS enn betra aðgengi að upplýsingum til að greina veigameiri erlenda aðgerðarhópa (e. advanced persistent threat groups) innan íslenskrar netlögsögu ásamt ítarlegri greiningu á helstu ógnarvísum. Það er mikilvægt fyrir sveitina að læra á og fullnýta þessar upplýsingar svo þær skili sem mestu virði fyrir Íslenska netumdæmið.




Erlent samstarf er CERT-IS gífurlega mikilvægt. Sveitin er virkur þáttakandi í norrænu samstarfi CERT teyma undir Nordic CERT Cooperation (NCC). Má greina mikinn kraft og vilja á þeim vettvangi að Norðurlöndin standi þéttar saman er kemur að netvarnarmálum. Ísland getur nú staðið jafnfætis frændþjóðum á slíkum vettvangi og skilað virði inn í samstarfið sem hægt að vera stolt af. Ísland á einnig í alþjóðlegu varnarsamstarfi við aðrar NATO þjóðir. NATO hefur skilgreint netárásir sem eina af mest vaxandi ógnum er steðja að aðildarlöndum og ólíkt raunlægari hættum í lofti, landi og sjó þá er í meira mæli undir aðildarlöndum sjálfum komið að tryggja að rétt sé staðið að netvörnum innan eigin landamæra. CERT-IS þakkar utanríkisráðuneytinu fyrir flott og faglegt frumkvæði við að tengja sveitina við mikilvæga samstarfsaðila innan NATO og tryggja þannig enn betur sameiginlega hagsmuni Íslands og bandalagsins.

Uppbygging CERT-IS hefur gengið vonum framar og erum við spennt fyrir komandi tímum. Nú má sjá fyrir endann á því þriggja ára ferli að koma netöryggisveitinni CERT-IS í fullan rekstur og leggja drög að áherslum næstu ára, íslenskum innviðum og almenningi til bóta.

Virðingarfyllst.
Guðmundur Arnar Sigmundsson
Sviðstjóri netöryggsveitarinnar CERT-IS

# Árið í tölum

Á hverju ári verða fjölmörg netöryggisatvik og er það hlutverk CERT-IS að halda úti tölfræði um hvaða atvik eiga sér stað í netumdæmi Íslands. Netöryggisatvik geta verið af ýmsum toga allt frá uppfærslu á tölvukerfum og rafmagnsleysi yfir í tækifærisárás tölvuglæpamanna eða markvissa og vel skipulagða árás á fyrirtæki eða stofnun.

Tölfræðin byggir eingöngu á atvikum tilkynntum til CERT-IS. Þar af leiðandi er gífurlega mikilvægt að tilkynnt sé um öll atvik sem upp koma. Tölfræðin gefur CERT-IS mikilvægar vísbendingar um hvernig þróun atvika er hér á landi sem aðstoðar við tilkynningar og ráðleggingar til stofnana, fyrirtækja og einstaklinga.

Eins og á síðasta ári er lang mest um netsvindl á Íslandi. Helst má sjá að þær herferðir sem herjuðu á Íslendinga árið 2022 voru vandaðri en áður. Tilkynningar um tilraunir til yfirtöku tvöfölduðust á milli ára. Þetta gefur vísbendingar um að oftar sé verið að reyna að brjótast inn í tölvukerfi á Íslandi. Það er engin leið að vita í raun hve oft reynt er að fremja netárás á fyrirtæki eða stofnanir enda margar tæknilegar varnir sem grípa flestar tilraunir til árásar án þess að eftir því sé tekið. Þegar upp kemst um tilraun til innbrota er árásaraðilinn kominn inn fyrir fyrstu varnir en er uppgötvaður áður en hann getur í raun valdið umtalsverðum skaða.

Þessi aukning er mögulegt áhyggjuefni. Aðeins þarf ein af þessum tilraunum að heppnast til að lama heilt fyrirtæki eða stofnun í styttri eða lengri tíma. Því þarf stöðugt að vera á varðbergi þegar kemur að vörnum tölvukerfa.

Fleiri tilkynningar um spillikóða eða óværur sem fundust í tölvukerfum á Íslandi bárust CERT-IS árið 2022. Spillikóðar eru búnir til af árásaraðilum og geta litið út fyrir að vera hættulausir þar til hann kemst inn í tölvukerfi. Óværur geta verið mismunandi en eru oftast notaðar til að eyðileggja gögn, taka yfir tölvukerfi eða við njósnir.

Að lokum er vert að nefna lítilega aukningu atvika vegna veikleika í tölvukerfum sem árásaraðilar eru að nýta sér. CERT-IS vekur athygli á þekktum alvarlegum veikleikum með tilkynningum á heimasíðu CERT-IS og einnig í gegnum póstlista sem hægt er að skrá sig á. Það er mikilvægt fyrir fyrirtæki og stofnanir að fylgjast með nýjum uppfærslum og framkvæma þær hratt og örugglega.

**8 atvik**

**Upplýsingatækni**

Aðgangur að upplýsigum eftir ólöglegum leiðum, gagnatap og gagnalekar.

**422 atvik**

**Svindl**

Netveiðar þar sem reynt er að komast yfir viðkvæmar upplýsingar, s.s. kortanúmer eða lykilorð.

**28 atvik**

**Veikleikar**

Veikleikar sem hægt er að nýta til að brjótast inn í eða hafa áhrif á tölvukerfi annarra.

**26 atvik**

**Spillikóði**

Tölvuveirur og annar kóði sem notaður er til að eyðileggja eða ná stjórn á tölvukerfum.

**15 atvik**

**Upplýsingasöfnun**

Söfnun upplýsinga um veikleika og netumferð án heimildar.

**26 atvik**

**Tiltækileiki**

Kerfi og þjónusta ekki aðgengileg af ytri ástæðum, t.d. álagsárásir þegar þjónusta tölvukerfa er vísvitandi skert með yfirálagi.

**9 atvik**

**Níðingsefni**

Einelti, áreitni og eltihrellni. Auk þess barnaníðsefni og upphafning ofbeldis.

**18 atvik**

**Innbrot**

Innbrot í tölvukerfi hjá heimanotendum, fyrirtækjum eða rekstraraðilum.

**34 atvik**

**Tilraun til yfirtöku**

Árangurslausar tilraunir til að taka yfir tölvukerfi fórnarlamba.

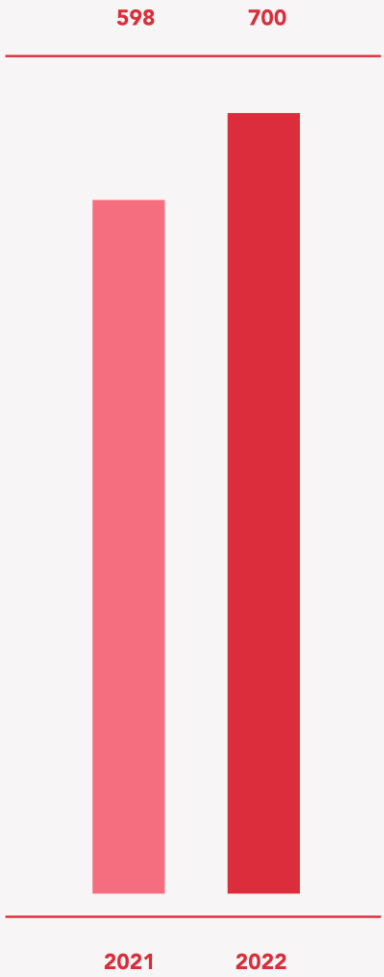
**114 atvik**

**Annað**

Aðburður sem ekki er hægt að flokka í ofangreinda flokka.

Samtals: **700 atvik**

## Tölfræði



# Vefveiðar

Nær öll þjónusta sem við þurfum er núorðið aðgengileg á netinu og rafræn skilríki auðvelda okkur það aðgengi. Áður fyrr þurfti að greiða reikningana sína í útibúi viðskiptabanka um hver mánaðamót en nú er bankaþjónusta að mestu aðgengileg í snjallforritum og á netinu.

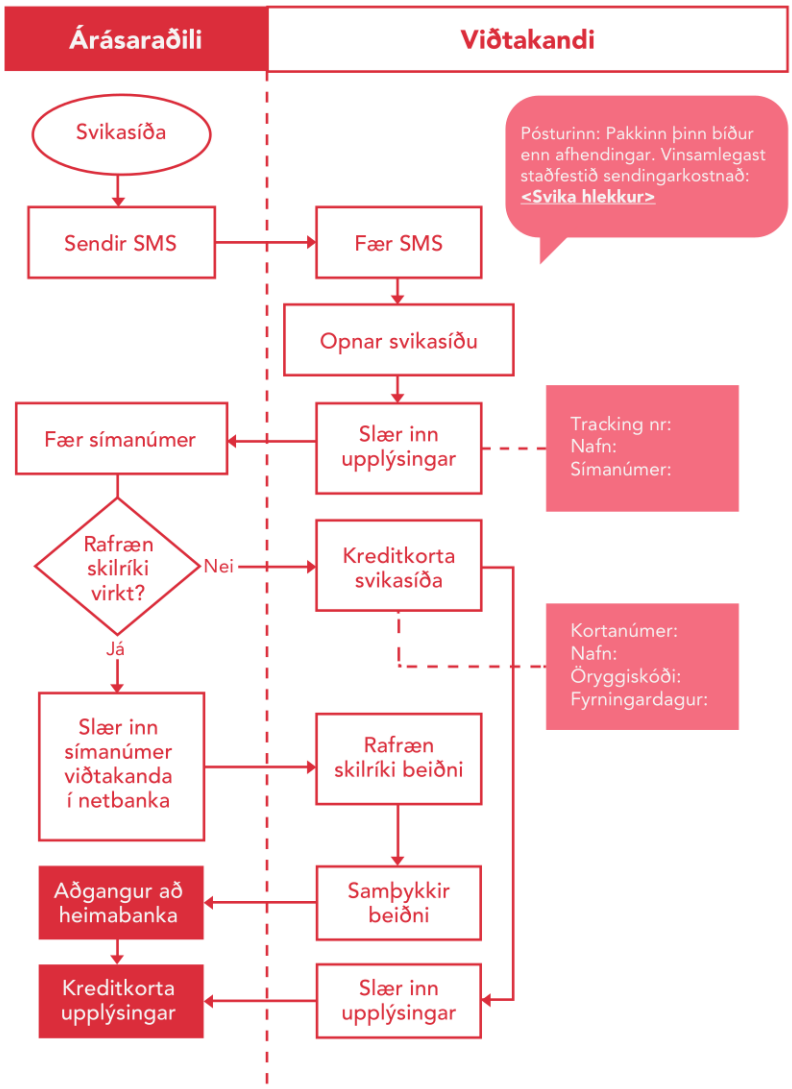
Undanfarin ár hafa vefveiðar færst í aukana. Óprúttnir aðilar eru viðstöðulaust að leita nýrra leiða til að svindla á fólki og breyta aðferðum sínum fljótt eftir því sem virkar best hverju sinni. Vefveiðar geta verið af ýmsum toga og beinst bæði að einstaklingum eða ákveðnu skotmarki t.d. fjármálastjóra tiltekins fyrirtækis.

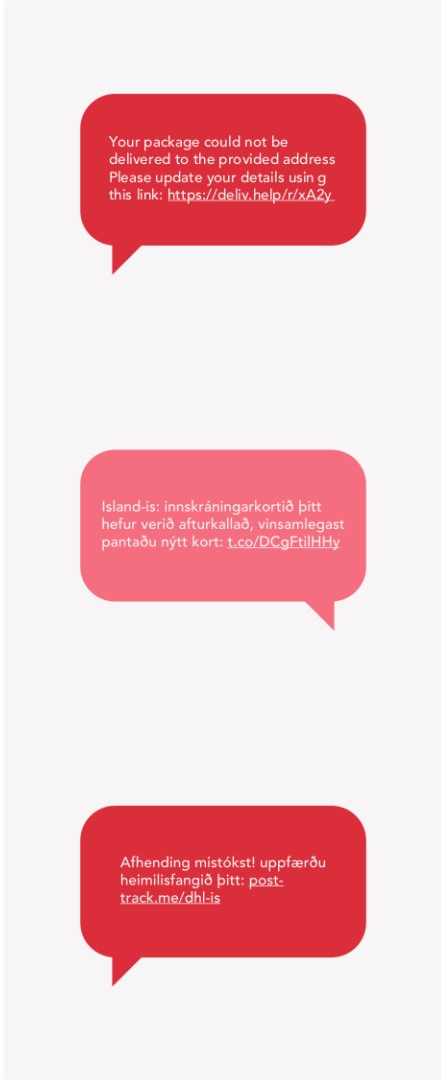
Óprúttnir aðilar nýta SMS skilaboð í miklum mæli í vefveiðum. Það er ýmislegt sem ýtir undir notkun þeirra. Opnunartíðni þeirra er mun hærri en vefpósta eða um 98% á móti 20%. Tíminn sem líður frá móttöku þar til opnunar skilaboðanna er að meðaltali ein og hálf mínúta fyrir SMS skilaboð en 90 mínútur fyrir vefpóst. Ofan á þetta leggst svo að einstaklingar eru tilbúnari til að treysta SMS skilaboðum frekar en vefpósti frá óþekktum aðila. Að lokum er til fjöldinn allur af öryggiskerfum og ruslsíum fyrir tölvupóstskerfi en ekki eins mikið fyrir SMS skilaboð.

Við könnumst flest við grunsamlega vefpósta. Þeir eru alla jafna illa samsettir og sérkennilega orðaðir. Búast má þó við breytingum þar á með tilkomu mállíkana eins og ChatGPT. SMS skilaboð eru einfaldari miðill en vefpóstar, yfirleitt stutt skilaboð með talnarunu eða hlekkjum og því kjörin leið fyrir árásaraðila til að villa á sér heimildir. Gjarnan er tekið fram að "sending þín hefur verið stöðvuð" eða "lokað hefur verið fyrir kortið þitt" og hlekkur látinn fylgja skilaboðunum sem viðtakandinn verður að smella á sem fyrst til að bregðast við.

Við smellinn er fyrsta markmiði árásaraðilans náð, að fanga athygli og veiða einstaklinginn á vefsíðu á sínum vegum. Þær síður biðja gjarnan um greiðslu smávægilegrar upphæðar svo hægt sé að afgreiða sendingu eða sýna upplýsingar um stöðu sendingar þar sem beðið er um nafn, heimilisfang og símanúmer. Í þessu samhengi eru þetta eðlilegar upplýsingar en það sem árásaraðilinn gerir á bak við tjöldin er að kanna hvort símanúmerið sé tengt rafrænum skilríkjum. Ef svo er ekki er beðið um kreditkortaupplýsingar en ef símanúmerið tengist rafrænum skilríkjum geta þau verið notuð til tilrauna til innskráningar í hvaða kerfi sem styðja það. Þetta geta verið heimabankar og þjónustusíður opinberra stofnana svo fátt eitt sé nefnt.

Í sumum herferðum er mikið lagt í uppsetningu á svindlinu og augljóst að mikil vinna hefur verið lögð í að kynna sér hvernig á að forðast eftirlit þeirra stofnana eða fyrirtækja sem eru misnotuð í svindlinu.




Það sem við getum gert til að verjast þessum svindlum er að staldra við og hugleiða trúverðugleika skilaboðana. Ef skilaboð eru sögð vera frá fyrirtæki eða stofnun má alltaf hafa samband við þær stofnanir beint og kanna raunmæti skilaboðanna. Símanúmerin okkar eru ekki lengur bara símanúmer og þetta vita árásaraðilar.

CERT-IS tekur á móti öllum vefveiðapóstum og skjáskotum af vefveiðum í smáskilaboðum á **phishing@cert.is**. Sendingar þangað aðstoða við að tryggja betri yfirsýn yfir svikapósta og herferðir sem beinast að Íslandi.

# Stríðið í Úkraínu

Þegar allsherjar innrás Rússlands í Úkraínu hófst í febrúar 2022 voru strax háværar raddir að samhliða hefðbundnum árásarleiðum myndu fylgja fjöldi tölvuárása á úkraínska innviði og jafnvel bandamenn Úkraínu. Árásirnar myndu koma frá rússneskum stjórnvöldum eða hópum hliðhollum þeim. Trúðu margir sérfræðingar að Rússar myndu nýta netárásir til að reyna að lama Úkraínu meðan á innrásinni stæði. Árið 2017 gerði Rússland einmitt það, lamaði daglegt líf í Úkraínu með skrúbb óværu (e.wiper) sem kallast NotPetya. Fjármálakerfi landsins lamaðist, spítalar misstu netsamband sem og flestar ríkisstofnanir í landinu. Óværan fór einnig langt út fyrir landamæri Úkraínu og hafði áhrif á fyrirtæki víða um heim, t.d. heilbrigðiskerfið í Bretlandi. Þó minna hafi farið fyrir tölvuárásum í fréttum í/af stríðinu en margir bjuggust við, hafa þær vissulega verið notaðar. Á fyrstu dögum stríðsins nýttu Rússar sér netárásir til þess að ýta undir óreiðu og skapa sundrung. Má þar nefna netárás á gervihnött, sem að hluta til tryggir samband innan úkraínska hersins, sem hófst klukkustund á undan innrásinni. Rússar beindu einnig spjótum sínum að heimasíðum ríkisstofnanna daginn eftir að innrásin hófst og að landamærastöðvum til að koma í veg fyrir fólksflótta. Auk þess nýttu Rússar sér djúpfölsun (e. Deep fake) af Zelensky, forseta Úkraínu, til að breiða út falsfréttum um að leggja niður vopn.

Það sem stendur upp úr er notkun skrúbb óværa á úkraínska innviði. Slík óværa var fyrst notuð árið 2012 og hafði verið beitt í það minnsta átta sinnum. Árið 2022 var skrúbb óværu beint þrettán sinnum að úkraínskum innviðum. Er það gríðarlegt stökk í notkun óværu sem aðeins er notuð til eyðileggingar, ólíkt öðrum árásarleiðum þar sem oft er hægt að endurheimta gögn að minnsta kosti í einhverri mynd.

Úkraínsk stjórnvöld kölluðu strax eftir aðstoð netöryggissérfræðinga bæði úr einka- og opinbera geiranum og létu viðbrögðin ekki á sér standa. Í fyrsta skiptið svo vitað er til eru netöryggisfyrirtæki til staðar í Úkraínu sem virkir þátttakendur í stríðsástandi að vinna með þarlendum stjórnvöldum.

Ef þú vilt fræðast meira um áhrif netárása á Úkraínu síðan innrásin hófst er ítarlegri grein að finna á heimasíðu okkar **www.cert.is**.

**14/2**
Ráðist á 70 ríkisstofnanir og birt „Wait for the worst" á heimasíðum þeirra

**24/2**
Ráðist á KA-SAT gervihnött

**25/2**
Ráðist á landamærastöðvar með skrúbb óværu

**4/3**
Ráðist á hjálparstofnanir innan Úkraínu

**16/3**
Ráðist á sjónvarpsstöðvar og djúpfölsun af Zelensky

**8/4**
Ráðist á orkugeira Úkraínu

**Þurrka** er óvær gerð til að hreinsa eða þurrka harða diskinn á tölvum. Eyðast þá öll gögn sem vistuð hafa verið og ekki hægt að nálgast þau aftur, nema afrit hafi verið geymt á ótengdri vél.

CERT·IS

# Netöryggi á Íslandi

Við upphaf innrásar Rússlands í Úkraínu breyttist öryggislandslag allrar Evrópu. Ísland hefur hingað til verið öruggara í hefðbundnum átökum en önnur lönd, verandi eyja í miðju Atlantshafi. Aftur á móti eru í dag breyttir tímar. Netið er án landamæra og öll ríki geta orðið fyrir netárásum.

Samhliða innrásinni í Úkraínu hafa Rússar og árásahópar hliðhollir þeim beitt tölvuárásum á innviði Úkraínu. Þeir hafa ekki látið kyrrt við liggja þar heldur beint tölvuárásum að aðilum hliðhollum Úkraínu í stríðinu. Sérstaklega hafa árásirnar beinst að núverandi og verðandi meðlimum Norður Atlantshafs-bandalagsins (NATO). Með aðildarumsóknum Finnlands og Svíþjóðar í NATO hefur athyglin beinst að Norðurlöndunum.

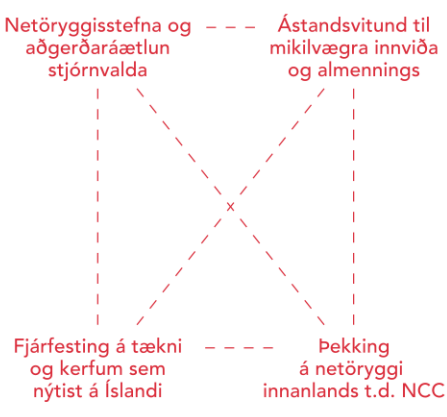
Öll Norðurlöndin hafa orðið fyrir árásum frá hópum hliðhollum Rússum. Dreifðar álagsárásir (DDoS) til þess að taka niður heimasíður og tímabundið lama starfsemi fyrirtækja eða stofnana eru þar algengastar. Á Íslandi sexfaldaðist skönnun á netumdæminu fyrstu vikurnar og mánuðina eftir að innrásin hófst borið saman við venjulegt ástand. Skönnun á netumdæmum er gerð í von um að finna veikleika sem hægt er að nýta í tölvuárásir. Oft er talað um að Ísland sé eftirbátur nágrannaþjóða í netöryggi. Til stuðnings þess er bent á lista frá Alþjóða Fjarskiptasambandinu (e. International Telecommunication Union eða ITU) þar sem Ísland er í 58. sæti listans. Þess ber þó að geta að sá listi var uppfærður síðast árið 2020 og hefur margt jákvætt gerst síðan þá.

Með innleiðingu NIS löggjafarinnar ásamt fjölgun starfsmanna CERT-IS hafa íslensk stjórnvöld bætt þjónustu við mikilvæga innviði. Ný netöryggisstefna fyrir Ísland var gefin út fyrir árin 2021-2036 og sérstök fimm ára aðgerðaráætlun til að sýna hvernig stjórnvöld ætla að ná markmiðum sínum í netöryggismálum umfram mikilvæga innviði. Þáttaskil urðu í netöryggismálum á Íslandi með stofnun NCC-IS sem er samstarfsvettvangur fræðslu, menntunar og rannsókna á netöryggi og farið verður að bjóða upp á meistaranám í netöryggi á Íslandi á næstu misserum. Áður fyrr hafði Ísland takmarkaða getu til að greina veigameiri erlenda aðgerðahópa (e. advanced persistent threat eða APT) sem mögulega herja á netumdæmi landsins. Í dag hefur CERT-IS gert samninga við aðila sem sérhæfa sig í greiningu á APT hópum og hefur þar af leiðandi aðgang að sérhæfðum tólum sem bæta greiningargetu CERT-IS til muna.

Þó margt hafi verið gert á síðustu árum er netöryggi aldrei tryggt að fullu. Netvarnir þarf sífellt að þróa í samræmi við breytta hegðun árásaraðila. Er því mikilvægt að fylgja vel eftir aðgerðaráætluninni til að tryggja að Ísland verði meðal fremstu þjóða í netöryggismálum.

Veigameiri erlendir aðgerðarhópar, **APT**, eru vel skipulagðir árásahópar, oft tengdir þjóðríkjum. Hóparnir sérhæfa sig í að komast óséðir inn í tölvukerfi þar sem þeir geta eyðilegt mikilvæga virkni í þeim eða stolið upplýsingum úr þeim til lengri tíma.

**Netöryggi á Íslandi skiptist á milli**



# Sviðshópar - hvað er gert og framtíðarsýn

Eitt af meginverkefnum netöryggissveitarinnar CERT-IS er að sinna mikilvægum innviðum og rekstraraðilum nauðsynlegrar þjónustu til að stuðla að betri viðbúnaði gagnvart netvá. Þannig hefur CERT-IS sett á fót þverfaglega samráðshópa fyrir þá innviði sem eru tilgreindir í lögum. Árið 2022 urðu þau tímamót hjá CERT-IS að hægt var að stofna og halda utan um alla sviðshópana, sem eru sex talsins og með yfir 50 rekstraraðila mikilvægra innviða og nauðsynlegrar þjónustu.

Markmiðið með sviðshópunum er fyrst og fremst að auðvelda upplýsingaskipti, auka ástandsvitund og að styrkja boðleiðir milli CERT-IS og mikilvægra innviða. Allir innviðir og þjónustur eiga það sameiginlegt að halda utan um og reka þjóðfélagslega mikilvægar þjónustur. Hópurinn er samt sem áður fjölbreyttur og með mismunandi þarfir og áhættur.

Fyrir suma innviði er mikilvægt að fá upplýsingar um kerfisuppfærslur og veikleika eða niðurstöður úr veikleikaskönnun sem CERT-IS hefur veitt. Hjá öðrum sviðshópum hefur athyglinni og umræðunni verið beint meira að starfsfólki og notendum þjónustunnar, þar sem árásarflöturinn er einmitt fólkið sjálft með vefveiðum og svikaherferðum. Það eru fjölmörg erlend dæmi um að stofnanir á borð við sjúkrahús og banka hafi lent í stórum árásum þar sem fyrsta skrefið inn í kerfin voru árangursríkar vefveiðar á starfsfólk.

**Sviðshópar**

**Orka**

**Heilbrigði**

**Veitur**

Markmiðið fyrir árið 2023 er að þróa enn frekar samstarfið gagnvart sviðshópum. Áætlað er að halda netöryggisæfingar til að styrkja boðleiðir milli þátttakenda í sviðshópunum og CERT-IS. Það verður fyrsta skrefið af mörgum í því að búa til skipulagðara fyrirkomulag netöryggisæfinga á Íslandi. Snemma veturs 2022 samþykkti Evrópuþingið og ráðið nýja tilskipun um öryggi net- og upplýsingakerfa mikilvægra innviða, sem ber heitið NIS2. Um er að ræða uppfærslu á þeim lögum sem CERT-IS starfar samkvæmt. Búast má við innleiðingu NIS2 tilskipunarinnar í íslensk lög árið 2024, og þar með muni fjölga í hópi þeirra innviða og rekstraraðila sem teljast bæði mikilvægir og nauðsynlegir.

Fjarskipti

Samgöngur


Fjármál

# Netöryggisæfingar

Netöryggisæfingar eru skipulagðar æfingar þar sem farið er yfir hvað á að gera ef ósamfella verður í rekstri net- og upplýsingakerfa. Dæmi um slíka ósamfellu í rekstri gæti verið allt frá því að kerfisuppfærslur geri mikilvæg kerfi óvirk um einhverja hríð upp í það að vera hrein og bein árás á upplýsingakerfi til dæmis með lausnargjalds- eða álagsárás.

Við könnumst öll við æfingar á borð við eldvarnaræfingar eða stærri flugslysaæfingar. Þar eru mismunandi sviðsmyndir teknar fyrir á skipulagðan hátt og viðbrögð og samskipti fjölmargra aðila æfð. Slíkar æfingar geta verið jafn einfaldar og að kveikja á eldvarnarkerfinu til að athuga hvort það virki upp í það að sviðsetja flugslys þar sem kveikt er í braki til að raungera tæknilega framkvæmd á vettvangi.

Netöryggisæfingar geta verið einfaldar skrifborðsæfingar þar sem viðbragð er samhæft, betur þekktar sem viðbragðsæfingar, upp í tæknilegar framkvæmdaræfingar þar sem tæknilegt viðbragð er raunprófað. Kjarninn í viðbragðsæfingum er að æfa boðleiðir og samskipti, því ef upplýsingar komast ekki hratt og rétt til skila, þá getur verið erfitt fyrir sérhæfða viðbragðsaðila að bregðast rétt við. Tæknilegar framkvæmdaæfingar einblína aftur á móti tæknilegt viðbragð við netvá í rauntíma þar sem "rauða liðið" er að framkvæma árás og "bláa liðið" þarf að verjast árásinni.

Netöryggisæfingin þurfa ekki að vera flóknar til þess að hægt sé að draga lærdóm af því hvernig eigi að bregðast við netvá. Oft eru svörin við spurningunum einföld, en stundum þarf að fylgja ákveðnum ferlum til þess að tryggja ekki einungis rekstrarsamfellu heldur einnig að lögum sé fylgt. Netöryggisæfingar snúast ekki bara um það að afstýra netvá, heldur einnig að lágmarka skaða sem hlýst af netvánni, flýta endurreisn og allt ferlið sem fer í gang eftir að atvik á sér stað.

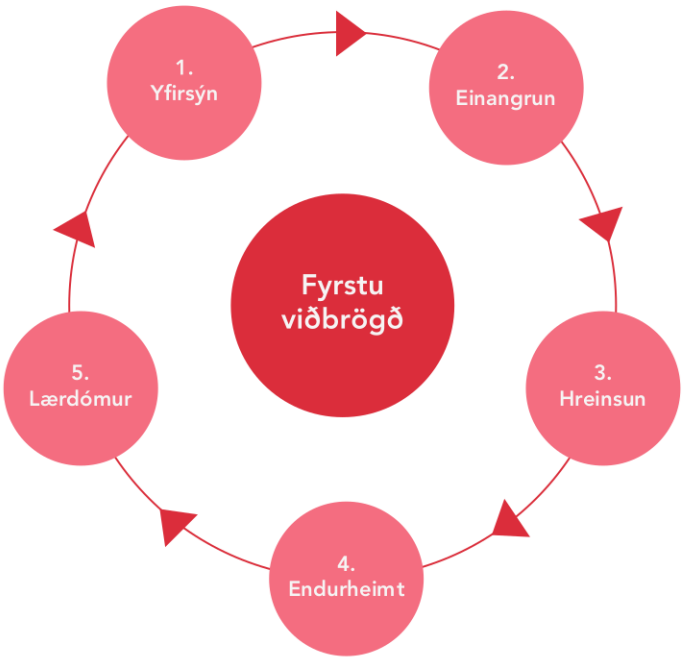
Þannig geta einfaldar skrifborðsæfingar þar sem viðbragð við netvá er samhæft gert mikið gagn til þess að prófa viðbragðsáætlanir og sjá hvar er hægt að gera betur. Það er ekki einungis tæknideildin sem þarf að koma að slíkri æfingu heldur einnig stjórnendur, lögfræðingar, mannauðsfulltrúar og fjölmiðlafulltrúar.

Markmiðið er að fara í gegnum ferlið frá upphafi til enda og geta svarað spurningunum á borð við

- Hvernig og hvenær varð atviksins vart?
- Hvernig var brugðist við atvikinu til að stöðva það?
- Hver var með yfirsýn og verkstjórn?
- Hvernig var upplýsingamiðlun háttað til stjórnenda og starfsmanna?
- Þurfti að tilkynna þetta til lögreglu, CERT-IS, Persónuverndar, eða annarra eftirlitsstjórnvalda? Ef svo er, hvernig var það gert?
- Hver var lærdómurinn af æfingunni?

Það er hægt að draga mikinn lærdóm af því að fara í gegnum eina sviðsmynd af netvá frá upphafi til enda með þeim hópi sem myndi koma að úrlausn atviks. Á heimasíðu CERT-IS er hægt að finna drög af einfaldri viðbragðsæfingu ásamt frekari upplýsingum um netöryggisæfingar.

Venja er að tala um „rautt lið" sem árásaraðilar í æfingum og eru að gera sitt besta til að ráðast á skilgreint fórnarlamb. „Bláa liðið" eru síðan þeir sem sinna tæknilegum aðgerðum í æfingum til að svara árásinni.



# Tímalína frá 2022

- Stríð brýst út í Úkraínu
- Sviðshópur orkuinnviða virkjaður
- DDoS Árás á Fréttablaðið
- Phishing@cert.is
- Ransomware árás á Tækniskólann
- Netöryggisæfing CERT-IS og SURF
- Netöryggismánuður
- Ný heimasíða með nýrri tilkynningagátt
- Sviðshópur heilbrigðisinnviða virkjaður
- Sviðshópur flutningainnviða virkjaður
- Aðgerðaáætlun stjórnvalda í netöryggi


CERT·IS