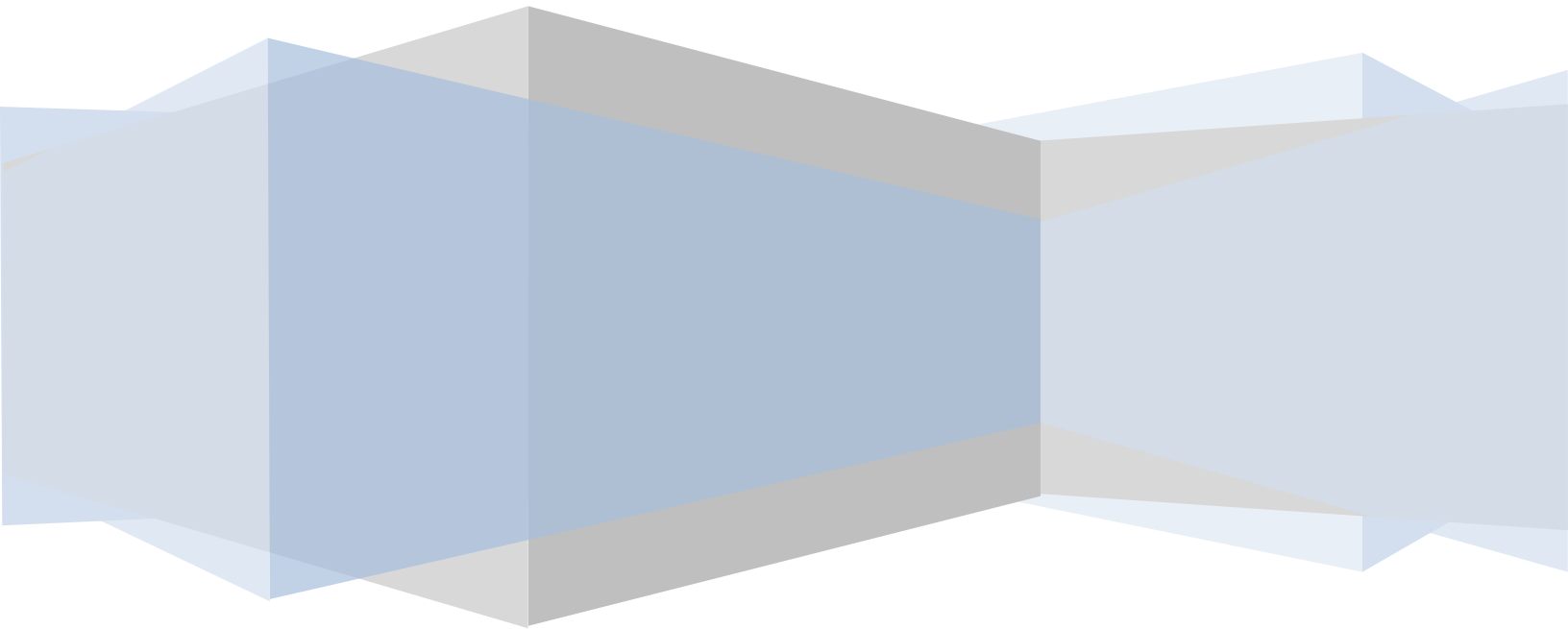
PÓST- OG FJARSKIPTASTOFNUN

Stofnun forystu CSIRT/CERT teymis á Íslandi gegn öryggisatvikum í fjarskipta- og upplýsinganetum

IceCERT

Kynningarskýrsla



ÁGÚST 2008

1 SAMANTEKT

- Hlutfallslega mikil netnotkun á Íslandi leggur þær skyldur á stjórnvöld að stuðla að betra öryggi Internetsins.

- Internetið ber uppi stöðugt meiri fjarskipti, á sama tíma og hættur þess fara ört vaxandi með tilheyrandi kostnaði. Meðan samhæfing aðgerða, samvinna og önnur reglufesta er ekki til staðar valda hætturnar og önnur yfirvofandi öryggisatvik[1] enn frekar beinu tekjutapi, fjárhagslegum kostnaði, óþægindum og hugsanlega töpuðum viðskiptatækifærum.

- CSIRT[2] teymi stuðla að vernd gagnvart fyrrgreindum ógnum. Þau eru starfandi víða í þjóðfélögum þeirra landa sem eru í kringum okkur. Yfirleitt er eitt CSIRT teymi í forystuhlutverki fyrir landið í heild sinni, annað hvort sem stjórnsýslu-CSIRT eða þjóðar-CSIRT.

- ESB lítur beinlínis á þjóðar- eða stjórnsýslu-CSIRT sem hornstein í vernd mikilvægra fjarskipta- og upplýsingainnviða í nánustu framtíð.

- Á Íslandi er ekkert CSIRT teymi með virka starfsemi starfandi í dag. Fjarskiptafyrirtækin hafa til þessa oftast brugðist við hvers konar ógnum hvert í sínu lagi, án allrar samhæfingar sín á milli.

- Niðurstaða skýrslunnar er að æskilegt sé að stofna þjóðar-CSIRT[3] til að berjast við vaxandi öryggisógnir í fjarskipta- og upplýsinganetum. Æskilegast er að slík forystuteymi stuðli bæði að vernd Internetsins á Íslandi, svo og annarra mikilvægra innviða í fjarskipta- og upplýsinganetum.

- Flest lönd sem Ísland ber sig almennt saman við eru með eitt forystu CSIRT í sínu landi. Starfsemin er yfirleitt frekar víðtæk, svo sem í Noregi, Danmörku og Svíþjóð. Finnland og Noregur eru með þjóðar-CSIRT en Holland er með stjórnsýslu-CSIRT (Governmental CSIRT). Slík flokkun er þó ekki alltaf afgerandi.

- Erfitt er að meta hversu miklum þjóðfélagslegum sparnaði rekstur CSIRT kemur til leiðar. Aðstæður og umhverfi taka sífelldum breytingum og mörg öryggisatvik reynast erfið viðureignar. Skv. nýjum tölum frá Bretlandi[4] nema árleg heildarútgjöld fyrirtækja þar í landi vegna öryggistvika um nokkrum milljörðum enskra punda. Einn milljarður punda samsvarar 17 enskum pundum á hvern Englending eða um 2,600 íslenskar kr. Því má leiða að því líkur að hvert prósentustig sem CSIRT stuðlar að minni áhrifum öryggisatvika, getur numið töluverðri upphæð hér á landi og eru þá ótalin útgjöld sem lenda beint á einstaklingum.

---

[1] Öryggisatvik er skilgreint sem „Atvik sem er gefið til kynna með einum eða fleiri óæskilegum eða óvæntum öryggisatburðum sem talsverðar líkur eru á að stofni rekstrarþáttum í hættu og ógni upplýsingaöryggi“. Hér er t.d. átt við berskjölduð upplýsingakerfi, netárásir, spilliforrit o.fl.

[2] Computer Security and Incident Response Team – „Teymi um tölvuöryggi og viðbrögð við öryggisatvikum“

[3] Í skýrslunni notum við heitið CSIRT (Computer Security and Incident Response Team - framb. “SíSört”) sem lýsir fyrirhugaðri starfssemi betur en eldra heitið CERT (Computer Emergency Response Team) þótt merkingin sé keimlík. Þjóðar-CSIRT er þýðing á „National CSIRT“.

[4] http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf

- Þjóðar-CSIRT hefur tiltekna hagsmunaaðila undir sínum verndarvæng, sem flestir reka stærri net- og tölvukerfi. Gerður er þjónustusamningur milli þjóðar-CSIRT teymisins og hagsmunaaðilana. Hagsmunaaðilarnir eru fyrst og fremst önnur verðandi íslensk CSIRT eða skilgreindar öryggisdeildir stærri fjarskiptafyrirtækja. Aðrir hagsmunaaðilar geta verið samtök minni fjarskiptafyrirtækja og vissir atvinnugeirar svo sem orkugeirinn. Ennfremur fyrirtæki og stofnanir með öfluga upplýsingastarfssemi; fjármálafyrirtæki, heilbrigðisstofnanir, löggjafarvaldið, háskólar og rannsóknarstofnanir.

- Þjóðar-CSIRT hefur bein tengsl við hagsmunaaðilana, en ekki við viðskiptavini þeirra, svo sem viðskiptavini banka og fjarskiptafyrirtækja. Það hefur ennfremur bein tengsl við erlend CSIRT og þá erlendu aðila sem þurfa að beina fyrirspurnum um öryggisatvik og aðvaranir til Íslands og tekur þátt í alþjóðlegri samvinnu við lausn þeirra.

- Þjóðar-CSIRT greinir og safnar saman gögnum um veikleika og berskjöldun í fjarskipta- og upplýsinganetum. Það varar hagsmunaaðilana við og ráðleggur um varnarráðstafanir. Teymið leggur áherslu á skjót viðbrögð, m.a. með að gefa út stuttar en markvissar ábendingar og viðvaranir til hagsmunaaðilanna, viðhafa sjálfvirkni við meðhöndlun öryggisatvika, samhæfa aðgerðir og skiptast á upplýsingum. Það flokkar gögn á sem skilvirkastan hátt og innleiðir stefnu og ferla sem eru auðskiljanlegar.

- Þjóðar-CSIRT leysir ekki öll vandamál af völdum öryggisatvika. Það er viðbót við aðrar núverandi varúðarráðstafanir í upplýsingatækni.

- Teymið þarf að vera með góð tengsl við fjölmiðla. Það miðlar og svarar fyrirspurnum þeirra um öryggisatvik líðandi stundar og öryggismál almennt. Hlutverk þess er þó ekki að svara fyrir einstakar bilanir og truflanir innan fjarskiptafyrirtækja.

- Traust er lykilatriði. Ef traust milli teymisins og hagsmunaaðilana brestur, t.d. ef starfssemin lamast vegna fjármagnsskorts, getur tekið langan tíma að endurvinna það og byggja upp aftur jákvæða ímynd þess.

- Margir telja óæskilegt að teymið fái bein fjárframlög frá hagsmunaaðilum sínum. Rökin eru þau að það sé sem minnst háð séróskum einstakra hagsmunaaðila við val á verkefnum og forgangi þeirra. Á móti kemur að greiðsla skapar oft tryggð við starfssemina.

- Í skýrslunni er gengið út frá því sem vísu að þjóðar-CSIRT teymið hafi líka hlutverk gagnvart öryggisatvikum sem upp kunna að koma í mikilvægum innviðum er varða þjóðaröryggi í fjarskipta- og upplýsinganetum í heild sinni. Þetta táknar að teymið sinni ekki eingöngu öryggisatvikum í tengslum við IP netkerfi og netþjónustu, heldur líka í öðrum fjarskiptakerfum svo sem almennum símnetum og farsímanetum. Sá þáttur fellur ágætlega undir starfssvið þjóðar-CSIRT.

- Skoða þarf hvort ástæða sé til að setja sérstakar reglur eða reglugerð til að skerpa rammann utan um fyrirhugaða starfssemi og samvinnu fjarskiptafyrirtækja við slíkt teymi.

- Áður en starfsemi hefst, þarf fjármögnunaráætlun og fjármögnun að vera frágengin.

- Reynsla annarra landa sýnir eftirfarandi;
  - ✓ Vanda þarf allan undirbúning og það tekur CSIRT teymi um 2 ár að hljóta viðurkenningu
  - ✓ Ef taka á skrefið til fulls þarf að lágmarki 4-5 starfsmenn til þjóðar-CSIRT í upphafi.
  - ✓ Það tekur um 8-9 mánuði að gera starfssemi virka eftir að starfsmenn eru ráðnir.
  - ✓ Töluvert er um ferðalög og ráðstefnur, og m.a. vegna sérhæfðrar þjónustu er sérmenntun og símenntun starfsmanna mikilvæg.
  - ✓ Það tekur um hálft ár fyrir nýjan starfsmann að verða virkur í starfi.

- **<u>Skýrsluhöfundur telur eftirfarandi hugmyndir helst færar í stöðunni:</u>**

A. <u>Þjóðar-CSIRT með frekar víðtæka starfssemi sem stuðlar að vernd gegn hættu í öllum almennum fjarskipta- og upplýsinganetum:</u>

- ✓ **Stofnkostnaður um 49 mj. kr. fyrsta árið**
- ✓ **Árlegur rekstrarkostnaður um 42 mj. kr. á ári (miðað við 5 starfsmenn í upphafi rekstrar)**
- ✓ **Þetta CSIRT stuðlar að vernd gegn hættu frá Interneti, í almennum símkerfum og í öðrum almennum fjarskiptanetum.**

B. <u>Þjóðar-CSIRT með frekar víðtæka starfssemi sem stuðlar að vernd gegn hættu í almennum IP fjarskiptanetum eingöngu (svo sem Internetinu):</u>

- ✓ **Stofnkostnaður um 41 mj. kr. fyrsta árið**
- ✓ **Árlegur rekstrarkostnaður 37 mj. kr. á ári (miðað við 4 starfsmenn í upphafi rekstrar)**
- ✓ **Þetta CSIRT stuðlar að vernd gegn hættu frá Interneti og öðrum almennum IP fjarskiptanetum eingöngu.**

C. <u>Þjóðar-CISRT sem starfrækir samhæfingarmiðstöð, þ.e. samhæfir aðgerðir um vernd gegn hættu í almennum IP fjarskiptanetum eingöngu (svo sem Internetinu):</u>

- ✓ **Stofnkostnaður um 30 mj. kr. fyrsta árið**
- ✓ **Árlegur rekstrarkostnaður um 26 mj. kr. á ári (miðað við 3 starfsmenn í upphafi rekstrar)**
- ✓ **Þetta er ódýrasta leiðin gagnvart hættu í almennum IP fjarskiptanetum eingöngu. Takmörkun starfsseminnar veitir veikari vernd gegn öryggisatvikum en fyrri leiðir. Á móti þarf teymið að treysta á aðstoð erlendra CSIRT um greiningu og lausn alvarlegra atvika, sem upp kunna að koma. Ekki er sjálfgefið að slík aðstoð fáist þegar stærri vandamál koma fram á heimsvísu.**

2 INNGANGUR

Stofnanir, fyrirtæki, háskólar og almenningur nýta sér í auknum mæli sveigjanleika og ódýr samskipti yfir Internetið, í stað hefðbundins pósts og síma. Internetið og aðrir innviðir fjarskipta- og upplýsinganeta eru orðnir þjóðfélaginu nauðsynlegir, á svipaðan hátt og vatns- og rafveita til landsmanna. Við þurfum að geta treyst á öryggi þeirra og þjónustu. Um leið og tækninni fleygir fram og framboð á þjónustu eykst, er öryggi og tiltækileika innviðanna jafnframt ógnað af sífellt nýjum áhættuþáttum. Stjórnun innviðanna færist á fleiri hendur og glufur og mistök eru gerð í hugbúnaði, sem spilltir netverjar nýta sér í fjárhagslegum tilgangi og netvopn verða skæðari. Skemmdarverk unnin með netvopnum geta skert þjónustu en netvopn spanna allt frá einföldum tölvuskipunum, til fjölþætts árásarhugbúnaðar sem auðvelt er að fá og auðvelt að beita án tillits til landamæra eða lögsögu. Ekki er líklegt að þessi þróun breytist á næstu árum og þurfa menn að vera í viðbragðs- og varnarstöðu, innanlands sem utan. Góð samskipti milli aðila skipta höfuðmáli, sem og greining vandamála sem upp koma og samræming aðgerða.

Undanfarin ár hafa CSIRT teymi gegn öryggisatvikum í upplýsingatækni verið sett á laggirnar erlendis. Teymin hafa það hlutverk að minnka líkur á að hagsmunaaðilar verði fyrir skakkaföllum á Internetinu.

Rætt hefur verið um að stofna forystu-CSIRT á Íslandi gegn öryggisatvikum í íslenskum netkerfum og netþjónustu. Markmiðið með þessari skýrslu er að kynna ávinning og tilkostnað við stofnun slíks teymis og er hún ætluð þeim sem taka ákvörðun um stofnun þess. Skýrslan veitir upplýsingar um mismunandi CSIRT útfærslur, um verkefni þeirra og hagsmunaaðila. Hún greinir hversu aðkallandi þjónusta slíks forystu-teymis er í nútíð og framtíð, ásamt greiningu á tilkostnaði og mati á ávinningi við stofnun þess á Íslandi að teknu tilliti til þeirra hættu sem steðjar að íslenskum netkerfum og netþjónustu.

Í skýrslunni er lýst því hlutverki sem forystu-CSIRT teymi hafa innan aðildarþjóða ESB, og fjallað um aukið hlutverk þeirra við vernd allra mikilvægra fjarskipta- og upplýsingainnviða Evrópu í nánustu framtíð.

Fjallað er um væntanlega starfssemi forystu-CSIRT í þremur útfærslum á starfsviði; CSIRT í samræmi við stefnu ESB um vernd fyrrgreindra innviði (þ.m.t. Internetið), CSIRT sem stuðlar að vernd Internetsins eingöngu, og að lokum takmarkaðasta starfssviðið sem samhæfingarmiðstöð einvörðungu.

Að lokum verður minnst lítillega á svokallaða viðvörunarhópa (WARP). Þeir gætu hentað þegar gerðar eru kröfur um enn minna umfang.

Til þess að fá sem besta innsýn og svör við óljósum atriðum, auk þess að mynda tengsl við rétta aðila, var farið í vettvangsferð til þjóðar-CSIRT teymisins í Finnlandi, „CERT-FI“ sem er rekið af eftirlitstofnuninni finnsku, FICORA. Haldin var dagskynning á starfseminni og hafa þeir lýst yfir þeim vilja sínum að aðstoða enn frekar við uppbyggingu CSIRT á Íslandi. GovCERT í Hollandi, sem er stjórnsýslu-CSIRT hollensku stjórnarinnar, hefur líka boðið fram aðstoð sína.

Eitt hlutverka ENISA (European Network and Information Security Agency) er að stuðla að stofnun CSIRT teyma innan ESB og EFTA. Sóttir voru árlegir vinnufundir með þeim um CSIRT málefni og einn svokallaður TF-CSIRT vinnufundur hjá TERENA (Trans-European Research and Education Association).

Fyrir hönd PFS, vann Stefán Snorri Stefánsson sérfræðingur í netöryggi að þessari skýrslu.

3 HÆTTUR Í ÍSLENSKUM NETKERFUM

INTERNETIÐ ER MARGBREYTILEGT EN JAFNFRAMT SVEIGJANLEGT. ÞÁ SEM TENGJAST ÞVÍ VANTAR OFT TÆKNIÞEKKINGU UM IP NET OG ÖRYGGISMÁL. ÚRELT EÐA RANGT UPPSETT STÝRIKERFI, VEIKLEIKI Í HUGBÚNAÐI, ÓSTIGBÆTT KERFI OG SKORTUR Á ÖRYGGISVITUND EINSTAKRA NOTENDA, MYNDAR GRÓÐRARSTÍU FYRIR ÓPRÚTTNA NETVERJA. ÞEIR EIGA AUÐVELT MEÐ AÐ KLÆÐAST DULARGERVUM, T.D. HYLJA HVAÐAN SAMSKIPTI ÞEIRRA EIGA UPPRUNA OG FELA HVERJIR ÞEIR ERU Í RAUN OG VERU. FYRIR UTAN HVERSU ÓDÝR SAMSKIPTI YFIR INTERNETIÐ ERU, ER AUÐVELT AÐ TENGJAST ÞVÍ OG FLAKKA UM ÞAÐ ÁN TILLITS TIL NOKKURRA LANDAMÆRA.

3.1 HÆTTUR SEM BLASA VIÐ Í ÍSLENSKUM NETKERFUM Í DAG:

Nýir aðilar er feta á braut tölvuglæpa í hagnaðarvon koma örast allra tölvuglæpamana fram á sjónarsviðið. Tæki og tól þeirra verða sífellt aðgengilegri og auðveldari í notkun sem gerir þessum sívaxandi hópi kleift að stunda þessa iðju. Ennfremur vex tölvuþrjótum ásmegin við hvers konar atlögur, skemmdarverk og njósnir á Internetinu. Skemmdarverk og árásir í fjárhagslegum tilgangi eru erfið viðfangs og fjölbreytileikinn eykst. T.d. er netárásarþjónusta í boði á internetinu, svokölluð DDOS árásarþjónusta. Söluaðilinn býður jafnvel ókeypis kynningu til að sýna fram á virknina, t.d. skjóta þeir niður tiltekinn vef á ákveðnum tíma. Slík þjónusta er hýst á botnet-sýktum vélum og er hægt að nota til þess að klekkja á keppinautum. Njósnir koma aðallega frá Norð-Austur Asíu og eru oftar en ekki styrktar af ríkisstjórnum þar. Ríki njósna um nágranna sína og er gömul hefð er fyrir slíkri starfsemi. Internetið hjálpar til við að gera þær áhrifaríkar og ódýrar. Að auki blasa m.a. eftirfarandi hættur við í íslenskum netheimum:

- Laumunet (Botnet/Zombies) eru algeng til að gera netárásir frá dreifðum upptökum (DDoSA), senda út ruslpóst (Bulk SPAM) eða grípa lykilborðsinnslátt (Keyloggers). Umferð frá laumunetum er farin að valda greinilegu álagi á Internetinu. Sjá nánar um þessa þætti:
    - Innlendir aðilar verða fyrir netárásum sem stundum eru það öflugar að þær hægja á útlandasamböndum netþjónustuveitnanna. Hvatinn að árásunum getur verið margvíslegur, m.a. að árásarmaðurinn telji sig eiga harma að hefna og beiti þessum leiðum til hefndar. Slíkar árásir koma oft niður á öðrum en þeim sem verður fyrir þeim, með hægara Internetsambandi til útlanda. Í þessum tilfellum reynir netþjónustuveitandinn að bregða upp síum og öðrum ráðstöfunum er minnkað geta áhrif árásarpakkanna. Oft er erfitt um netvarnir og varir truflun á meðan árásin gengur yfir. Netþjónustuveitendur þurfa hugsanlega að leita til utanaðkomandi forystu-CSIRT ef stórtæk árás dynur yfir.
    - Ruslpóstur “Bulk spamming” sem berst að utan er vandamál sem fyrir utan óþægindi hjá notendum, getur valdið verulegu umferðarálagi á íslensk netkerfi og netþjónustu. Hætta er á að hann trufli virkni þeirra. Í verri tilfellum þarf að samhæfa aðgerðir og gæti CSIRT aðstoðað í þeim efnum.
    - Vafasöm spilliforrit sem grípa lykilborðsinnslátt óséð, svokallaðir “Keyloggers”, stofna öryggi upplýsinga í tölvukerfum í hættu er þau senda upplýsingarnar áfram til tölvuþrjóta. Þessi forrit eru í stöðugri þróun og þarf að veita þeim viðnám. Hlutverk CSIRT-teyma er m.a. að rannsaka mál af þessu tagi, veita viðvörun og benda á ráð til að finna slík spilliforrit og verjast þeim.
- Óprúttnir aðilar í útlöndum hafa náð að skerða þjónustu nokkurra megin nafnaþjóna á Internetinu. Einn slíkur þjónn er staðsettur á Íslandi og hefur hann sloppið til þessa. Þungamiðjan í starfssemi CSIRT er öryggi Internetsins og gætu þeir komið inn í þessi mál, ef svo ber undir.

- Internetið er ein heild, og þess vegna má segja að hvers konar aðrar truflanir á Internetinu teygi anga sína á vissan hátt til Íslands, þótt vandamálið eigi upptök sín í öðrum netkerfum. Dæmi um þetta eru veirur sem berast víða og staðbundin truflun sem hefur áhrif að alla umferð sem þar er beint í gegn. Alvarlegar truflanir á Internetinu koma inn á borð CSIRT, bæði þess teymis sem netkerfið tilheyrir (ef slíkt teymi er til staðar) og samstarfsteyma þess svo sem forystu-CSIRT viðkomandi lands.

3.2 STÆRRI OG MEIRI ÓGNIR SEM LÍKLEGT ER STEÐJI AÐ Í NÁINNI FRAMTÍÐ

3.2.1 AUKIN BANDBREIDD TIL ÍSLANDS

- Nú er unnið að því að bæta við þriðja sæstrengnum til Íslands. Slíkur strengur bætir vissulega samskipti okkar við önnur lönd en aukin flutningsgeta hefur líka sinn annmarka. Við aukna flutningsgetu aukast möguleikar óprúttinna aðila, eða þeirra sem telja sig eiga harma að hefna, til að vinna skemmdarverk á vefsetrum og öðrum tölvubúnaði á Íslandi. Skemmdarverkin gætu verið unnin með DDoSA netárás, sem getur verið erfitt að glíma við. Fram til þessa hefur flutningsgeta sæstrengja til Íslands að vissu leyti verið heftandi gegn því að slíkar árásir verði verulega máttugar. Aukin flutningsgeta stuðlar aftur á móti að því að árásarnir geta orðið öflugri og valda um leið meiri truflunum á þjónustu. Sem dæmi má taka um hugsanlega hættu á þjónustuskerðingu;

    - Hópur utanlands, sem er ósáttur við stefnu íslenskra stjórnvalda, t.d. í virkjunarmálum, eða annarri nýtingu auðlinda, svo sem í fisk- og hvalveiðum, gerir DDoSA netárás á vefsíður stjórnvalda, þjónustusíður framkvæmdaaðila, verktaka og undirverktaka.

    - Sú hætta er fyrir hendi, sama hver tilgangurinn væri, að gerð sé árás á netbanka eða vefsíður skattamála m.a. rafræn skattskil, eða hvers konar aðra þjónustu svo sem hugsanlegra netkosninga.

    - Sumir erlendir stjórnmálamenn hafa rætt um að hefðbundin stríð séu tímaskekkja. En deilur milli landa munu halda áfram og er sá möguleiki ekki útilokaður að netárása-“stríð” verði háð á Internetinu með stórtækum truflunum netkerfa víða um heim. Talið er að leyniþjónustur nokkurra landa tengist nú þegar slíkum málum. Netöryggi snertir ekki lengur fyrirtæki og einstaklinga eingöngu, heldur varðar þjóðaröryggi ríkja.

    - Við slíkar kringumstæður þarf að samhæfa varnir í íslenskum netkerfum og gefa net- og þjónustuveitum ráð. Forystu-CSIRT teymum er m.a. ætlað slíkt hlutverk.

3.2.2 GAGNAVER

Rætt er um að setja upp gagnaver, sem virkar sem afar stór gagnagrunnur fyrir erlend stór tæknifyrirtæki. Ekki er ólíklegt að slík ver yrðu rekin á íslenskum netkerfum, sem okkur ber að vernda.

3.2.3 SPILLIFORRIT

Spilliforritum er plantað óumbeðið í tölvur með sífellt flóknari tækni og leiðum. Veiruvarnir og varnir gegn njósnahugbúnaði hafa oft gert ágætis gagn til þessa. En spilliforritin eru í örri þróun og nú er svo komið að varnarforritin finna ekki viss spilliforrit sem plantað er í djúpt niður í stýrikerfi tölva, svokölluð rótarmein (Rootkit). Þau leynast ansi vel og þarf sérhæfð forrit við leit að þeim, ef þau á annað borð finnast. Áður fyrr ollu spilliforritin skemmdum í búnaði og usla meðal netnotenda. Í dag hafa þau þann aðaltilgang að

afla fjár á ósvífinn hátt með margbrotnum aðferðum til að notfæra sér veikleika í tölvum. Þetta á eftir að aukast og erlendis er þróunin sú að spilliforrit, sem undanfarin ár var eingöngu beint gegn notendum stærri banka, eru orðin sérhæfðari og minni bankar verða líka fyrir barðinu á þeim. Íslenskir bankar og viðskiptamenn þeirra hafa verið tiltölulega óhultir hingað til, aðallega vegna smæðarinnar, en teikn eru á lofti um að það gæti breyst. Ef spilliforrit færi í umferð hér sem nýtti sér aðgang að fjármagni gegnum veikleika í tölvum á Íslandi, þarf að bregðast við á markvissan hátt og er það eitt af hlutverkum CSIRT teyma.

3.2.4 LAUMUNET (BOTNET)

Margir telja að nú sé öld laumunetanna (Botnet) rétt að byrja. T.d. telur Europol þau mestu ógnina sem vofir yfir netheimum í dag. Nýjustu laumunetin eru mjög skæð því þau breyta ótt og títt um nöfn vélanna sem hýsa þau (DNS nöfn), sem gerir það að verkum að afar erfitt er að leita þau uppi og loka þeim. Svæsnustu laumunetin gera netárás á þann aðila sem reynir að uppræta þau. Vel útbúin CSIRT teymi rannsaka laumunet og önnur alvarleg spilliforrit og veita viðvaranir gegn þeim. Þau birta ráðleggingar sem má miðla áfram til almennings.

Dæmi um afurð laumunetanna er söfnun lykilorða berskjaldaðra Íslendinga þegar þeir tengjast þjónustuvefjum, svo sem í bankageiranum. Lykilorðin væri hægt að birta á opinni vefsíðu í útlöndum til að klekkja á almenningi hér heima.

3.2.5 ÖNNUR VÁ

- Vá sem stafar staðbundið að íslenskum netkerfum, gæti orðið það erfið viðureignar að hún verður ekki leyst hér heima. Í slíkum tilfellum er þörf á lausn með alþjóðlegri samvinnu CSIRT teyma og annarra hluteigandi aðila. Íslenskur forystu-CSIRT gæti verið milligönguaðili, t.d. milli rekstraraðila íslenskra netkerfa og -þjónustu og erlendra CSIRT teyma, fyrirtækja og stofnana.
- Ófyrirséðir veikleikar hafa komið fram innan nettækninnar sem tölvuþrjótar hafa nýtt sér og sú hætta líður ekki hjá. Ef upp kemur sú staða að Internetinu í heild sinni er ógnað á einhvern hátt, þá þurfa hérlendir aðilar að stilla saman strengi sína við útlenda CSIRT. Eðlilegt er að slíkt kæmi í hlut innlends forystu-CSIRT. Samvinna við önnur CSIRT er mikilvægur þáttur í starfsemi sérhvers CSIRT teymis.

4 ÞJÓÐFÉLAGSLEG ÁHRIF EF EKKERT VERÐUR AÐHAFST

Kostnaður fyrirtækja og hins almenna netnotanda vegna öryggisatvika á Internetinu fer sívaxandi. Í dag vegur kostnaður af völdum þjónusturofs meira en bein útgjöld við varnir og viðgerðir. Þar fyrir utan eru margs konar óþægindi sem öryggisatvik og hætta á þeim valda.

Talið er að árið 2005 hafi sú sláandi umbreyting orðið, að veltan í tölvuglæpaheiminum varð hærri en í eiturlyfjaheiminum. Þar er átt við þær tekjur sem netglæpamenn hafa upp úr alls konar svikastarfssemi í Internetinu.

4.1 BEINT TEKJUTAP

Erfitt er að meta hversu miklum þjóðfélagslegum sparnaði rekstur CSIRT kemur til leiðar. Aðstæður og umhverfi taka sífelldum breytingum og mörg öryggisatvik reynast erfið viðureignar. Nýleg könnun „2008 Information Security Breaches Survey[5]“, sem var gerð á vegum www.security-survey.gov.uk í Bretlandi, af PriceWaterhouseCoopers, gefur til kynna að árleg heildarútgjöld fyrirtækja þar í landi vegna öryggisatvika nemi um nokkrum milljörðum enskra punda. Einn milljarður punda samsvarar 17 enskum pundum á hvern Englending eða um 2,600 íslenskum krónum.

Reikna má með að íslenskt tækniumhverfi sé sambærilegt við það breska. Því má leiða að því líkur að hvert prósentustig sem CSIRT stuðlar að minni áhrifum öryggisatvika, getur numið töluverðri upphæð til sparnaðar hér á landi og eru þá ótalin þau útgjöld sem lenda beint á einstaklingum.

4.2 TÖPUÐ VIÐSKIPTATÆKIFÆRI

Ef öryggi er lakara á Íslandi en í nágrannalöndunum er hætt við að aðilar, svo sem erlendir bankar, netþjónabændur og aðrir sem þurfa að treysta á sem öruggasta tækni, flytji starfsemi sína síður til Íslands. Jafnframt er viss hætta á að íslensk fyrirtæki flytji frekar starfsemi sína til útlanda.

Sú staða gæti komið upp að útlend fjármálaeftirlitsstofnun ályktí sem svo að öryggi í íslenskum bankaheimi fullnægi ekki öllum þeirra kröfum vegna skorts á forystu-CSIRT hérlendis sem m.a. stuðli að auknu tölvuöryggi í fjármálageiranum.

[5] http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf

5 FORSAGA CSIRT TEYMA OG NÚVERANDI STARFSEMI

5.1 FORSAGAN

Í árdaga Internetsins voru fáir notendur sem báru traust hver til annars. En með aukinni notkun varð smátt og smátt breyting þar á. Árið 1978 var fyrsti ruslpósturinn sendur til allra sem höfðu netföng a Internetinu. Tíu árum síðar verða stór kaflaskil þegar fyrsta spilliforritið náði útbreiðslu á Internetinu í líki Morris tölvuormsins. Þá strax áttuðu menn sig á nauðsyn þess að bregðast við slíkum öryggisatvikum í framtíðinni. Mikilvægt þótti að kerfisstjórar, forstöðumenn tölvudeilda og fleiri aðilar ynnu saman og samhæfðu varnaraðgerðir til að kljást við þessi mál. Skömmu seinna var CERT/CC[6] (CERT Coordination Center) neyðarteymi/samhæfingarmiðstöð stofnuð í Bandaríkjunum, sú fyrsta í veröldinni. Frá upphafi var ljóst að eitt teymi réði ekki við margbreytileg öryggisatvik í sívaxandi netkerfum og fylgdu önnur neyðarteymi í kjölfarið um heim allan.

Starfsemi CERT neyðarteymanna var upphaflega nær eingöngu fólgin í neyðarviðbrögðum við þeim aukna fjölda öryggisatburða í Internet-tengdri upplýsingatækni, sem fylgdu í kjölfar Morris tölvuormsins. Fljótlega varð starfsemi slíkra teyma víðtækari með aukinni rækt við forvarnir, t.d. greiningu á hættunni sem fylgdi aðsteðjandi ógnum, þjálfun og þekkingarmiðlun, auk áherslu á samvinnu og upplýsingaskipti við önnur hliðstæð teymi. Skammstöfunin CERT, þ.e. “neyðarteymi í upplýsingatækni”, endurspeglaði því ekki lengur starfsemina og fóru menn að tala um CSIRT (Computer Security and Incident Response Team) sem þótti endurspegla betur tilgang þeirra; að sinna forvörnum, vera í viðbragðsstöðu og aðstoða hagsmunaaðila sína með viðbrögð gegn gegn netvá, ekki aðeins á Internetinu heldur hugsanlega líka í öðrum fjarskipta- og upplýsinganetum. Enn frekar ýtti sú staðreynd undir nafnabreytinguna að CERT nafnið er skráð vörumerki Carnegie Mellon háskólans í Bandaríkjunum, sem enn í dag rekur fyrrgreint CERT/CC sem ber höfuð og herðar yfir önnur CSIRT teymi í Bandaríkjunum og víðar. Það þótti því ekki við hæfi að nota það almennt sem samheiti yfir slík teymi, þótt það heyrist ennþá við og við, sérstaklega í talmáli manna á milli.

Með fjölgun CSIRT teyma í flestum löndum, var farið að samhæfa starfsemi þeirra undir einu forystu-CSIRT teymi í hverju landi.

Að gömlum sið inniheldur heiti margra CSIRT í heiminum “CERT” skammstöfunina, t.d. “SURFnet-CERT” sem var fyrsta CSIRT teymið í Evrópu, stofnað 1992 í Hollandi. Í dag eru milli 100 til 200 CSIRT teymi starfandi í Evrópu. Ef “CERT” er hluti af heiti þeirra, þá aðgreina þau sig með öðru auðkenni, t.d. CERT-DK, CERT-FI o.s.frv.

Í þessari skýrslu notum við frekar heitið „CSIRT“ í stað „CERT“ en í raun er meiningin nokkurn veginn sú sama. - Í leiðinni er rétt að geta þess að ESB hefur notað „CERT“ heitið en stundum „CSIRT“ eða „CERT/CSIRT“. ENISA notar í sínum gögnum nær eingöngu heitið „CSIRT“ yfir þessa starfsemi.

5.2 STARFSEMI CSIRT Í DAG

[6] Ennþá í dag er CERT/CC leiðandi og stefnumótandi fyrir önnur CSIRT teymi í veröldinni, auk þess að leitast við að vera í fararbroddi með tilkynningar öryggisatvika.

CSIRT eru starfandi í ýmsum atvinnuvegum sem hrein viðbót við hverskonar aðra öryggisstarfsemi sem er til staðar. Starfsemi CSIRT í dag má skilgreina á eftirfarandi hátt:

"CSIRT bregst við atvikum varðandi tölvuöryggi með því að veita nauðsynlega þjónustu til að leysa málið eða styðja þá lausn sem þegar er fundin. Teymið reynir að koma í veg fyrir öryggisatvik af þessu tagi innan síns áhrifasvæðis".

Segja má að hvatinn að stofnun CSIRT í dag mótist af eftirfarandi:

- Almenn fjölgun þeirra sem verða fyrir barðinu á öryggisatvikum.
- Sú staðreynd að kerfis- og netstjórar einir og sér ráða ekki við stærri öryggisatburði er upp kunna að koma.
- Vitund stjórnenda fyrirtækja um mikilvægi öryggisstefnu og verklags sem hluta af heildar áhættustjórnun fyrirtækisins hefur aukist.
- Ný lög og reglur sem leggja skyldur á fyrirtæki um vernd upplýsingakerfa.

Verkefni CSIRT eru almennt eftirfarandi:

- Hagsmunaaðilar geta leitað til CSIRT sem miðpunkts samhæfingar gegn öryggisatvikum í fjarskipta- og upplýsingakerfum sínum.
- CSIRT bregst kerfisbundið við slíkum öryggisatvikum og grípur til viðeigandi ráðstafana.
- CSIRT aðstoðar hagsmunaaðila sína á skjótan og árangursríkan hátt við að koma hlutunum í samt lag eftir að öryggisatvik hefur komið upp og heldur tjóni vegna þjófnaðar á upplýsingum eða rofi á þjónustu í lágmarki.
- CSIRT hagnýtir sér uppsafnaðar upplýsingar við hvert öryggisrof til að byggja upp betri varnir fyrir tölvukerfi og upplýsingar.
- CSIRT bregst á réttan hátt við þegar lagaleg atriði koma upp í tengslum við öryggisatvik.
- CSIRT leggur áherslu á að hagsmunaaðilarnir deili með sér þekkingu um öryggismál.
- Ímynd hagsmunaaðilana styrkist í tæknilegu og markaðslegu tilliti.

Það er mikilvægt að ítreka að CSIRT eru hrein viðbót við það skipulag öryggismála sem fyrir er. Þau leysa ekki af hendi mikilvægan viðbúnað gegn ósamfelldum rekstri fjarskipta- og upplýsinganeta, né starfsemi björgunarsveita eða lögreglu á nokkurn hátt.

5.3 CSIRT ÁHRIFASVÆÐI (CONSTITUENCY)

CSIRT er nokkurs konar verndari á sínu áhrifasvæði, þar sem teymið leggur mesta áherslu á forvarnir og viðbrögð gegn öryggisatvikum í fjarskipta- og upplýsingatækni sem tengjast einum eða fleiri hagsmunaaðilum.

„Á CSIRT áhrifasvæði eru þau fjarskipta- og upplýsingakerfi sem teymið stuðlar að betra öryggi í, og/eða hagsmunaaðilarnir sem nota kerfin og stýra þeim".

Í skýrslunni vísum við oftar en ekki á svæðið sem tæknikerfi en stundum sem hagsmunaaðila.

Dæmi um CSIRT áhrifasvæði í útlöndum eru t.d. háskólanet, iðnaðargeirinn, almenningur og stjórnvöld. Ennfremur reka fleiri og fleiri einstakir einkaaðilar CSIRT fyrir sína eigin starfssemi, svo sem hátæknifyrirtæki, bankar og fjármálafyrirtæki.

5.4 HAGSMUNAAÐILAR

Eins og fyrr segir eru hagsmunaaðilarnir þeir aðilar sem njóta þjónustu tæknikerfanna innan CSIRT áhrifasvæðisins. T.d. ef Internet-tengt upplýsingakerfi tiltekins banka er á áhrifasvæði CSIRT teymis, er bankinn í heild sinni hagsmunaaðili. Viðskiptavinir banka eru aftur á móti hagsmunaaðilar bankans en ekki CSIRT teymisins.

5.5 DÆMI UM HVAÐ CSIRT GERIR EKKI

Til að koma í veg fyrir misskilning skal tekið fram að CSIRT er ekki:

- Vírusvarnar-fyrirtæki.
- Teymi sem sinna veikleika-rannsóknum í hugbúnaði og kerfum.
- Teymi sem stundar glæparannsóknir í tengslum við tölvumál.
- Ábyrgt fyrir eigin upplýsingaöryggi annarra.

6 AÐKOMA HINS OPINBERA, HLUTVERK PFS OG TILMÆLI ESB

Á Íslandi er í dag ekkert CSIRT teymi með virka starfsemi. Fjarskiptafyrirtækin hafa til þessa oftast brugðist við hvers konar ógnum hvert í sínu lagi, án allrar samhæfingar milli sín. Þegar áðurgreind vá er skoðuð má draga þá ályktun að æskilegt sé bregðast við með stofnun CSIRT forystu-teymis. Teymið ráði starfsmenn sem hafa viðhlítandi menntun, þjálfun, þekkingu og skilning á áhættu og öðru tengt öryggisatburðum í fjarskipta- og upplýsinganetum svo sem Internetinu, auk þekkingar á ógnum og árásum á berskjölduð netkerfi og netþjónustu sem veitt er á Íslandi.

6.1 FJARSKIPTAÁÆTLUN 2005-2010

Með þetta að leiðarljósi hafa stjórnvöld lýst yfir vilja sínum í tengslum við CSIRT/CERT á Íslandi í eftirfarandi samþykkt Alþingis og skýrslu samgönguráðuneytis:

- Alþingi samþykkti á sínum tíma fjarskiptaáætlun 2005-2010 þar sem m.a. stendur skrifað:
  - "Að stofnaður verði CERT-hópur (Computer Emergency Response Team) [7] til að herða viðbrögð vegna óværu á Internetinu (grein 3.3.5 bls. 27)".
  - "Þátttaka Íslendinga verði aukin í erlendu samráði um öryggismál og varnir efldar til að net- og upplýsingakerfi virki óhindrað (grein.4.5.5 bls.57)".
  - Ábyrgð: Póst- og fjarskiptastofnun

6.2 SKÝRSLA STARFSHÓPS SAMGÖNGURÁÐHERRA UM ÖRYGGI FJARSK. O.FL. FRÁ NÓV. 2006

- **Bls. 5 – "Samstarf opinberra aðila og markaðarins um öryggismál verði eflt.** Póst- og fjarskiptastofnun hafi frumkvæði að því að koma á og skipuleggja CERT samstarf. Stofnunin annist slíkt samstarf, leggi til nauðsynlega aðstöðu og sjái um samráð við aðrar stofnanir ríkisins. (3.8) - **Ábyrgð:** Póst- og fjarskiptastofnun".
- **Bls. 14 - "Leggja verður áherslu á að byggja upp traust á upplýsingasamfélaginu, öryggi innviða þess og samkeppnishæfni.** Nauðsynlegt er að auka samvinnu, "miðlun upplýsinga og samstarf milli opinberra aðila og aðila á markaðinum um öryggismál, m.a. með því að samræma stefnu, ábyrgð, markmið og þannig ná betri árangri og hagnýtingu fjármuna við framkvæmd öryggismála. Þá má lágmarka áhrif utanaðkomandi ógna eða atburða með markvissu samstarfi og samvinnu í viðbrögðum m.a. í gegnum CERT-hópa".
- **Bls. 22 - CERT-skipulag, viðvörunarskipulag** "Aðkoma opinberra aðila að CERT-málum verði fólgin í yfirumsjón með því að aðilar sem veita netþjónustu sinni sameiginlegum öryggishagsmunum á skipulegan hátt. Samhæfa þarf viðbrögð þeirra rekstraraðila sem veita þjónustu við útlönd og koma boðum til CERT-aðila erlendis".

[7] Sama og CSIRT teymi

- Ennfremur í sömu skýrslu um þá innviði net- og upplýsingakerfa er varða þjóðaröryggi:

    - **Bls. 5 – "Auðkennd verði þau net- og upplýsingakerfi er varða þjóðaröryggi.** Þau tekin út á grundvelli áhættu og veikleikagreiningar og öryggi þeirra samhæft. Ábyrgðaraðilar hvers kerfis tryggi öryggi þess. Komið verði á samstarfi ábyrgðaraðila við almannavarnaryfirvöld. (3.9.) **Ábyrgð:** Dóms- og kirkjumálaráðuneyti, Ríkislögreglustjóri, Póst- og fjarskiptastofnun".

    - **Bls. 5 – "Komið verði á fót nefnd til að huga að öryggi kerfa er varða þjóðaröryggi.** Nefndin hafi formleg tengsl við almannavarnir eða Almannavarnaráð. Nefndin hafi samstarf við CERT-hópinn. (3.9). **Ábyrgð:** Dóms- og kirkjumálaráðuneyti, Ríkislögreglustjóri, forsætisráðuneyti".

6.3 REGLUR PÓST- OG FJARSKIPTASTOFNUNAR NR 1223/2007

Með ofangreint markmið stjórnvalda að leiðarljósi voru sett ákvæði um upplýsingaskyldu fjarskiptafyrirtækja gagnvart CSIRT í reglum Póst- og fjarskiptastofnunar nr. 1223/2007 um "Vernd, virkni og gæði IP fjarskiptaþjónustu", 25. gr. sem hljóðar svona;

✓ *„Í þeim tilgangi að auka heildstæði og öryggi fjarskiptaneta, skulu fjarskiptafyrirtæki taka þátt í samstarfi við öryggishópa[8] gegn vá í fjarskiptanetum og upplýsingakerfum á Íslandi, m.a. með því að senda til þeirra gögn um öryggisatburði, öryggisatvik, ósamfellda virkni og tortryggileg atvik, sem geta valdið truflunum á samfelldri þjónustu eða sett þjónustu og gögn viðskiptavina í hættu. Póst- og fjarskiptastofnun, eða sú samræmingarstöð öryggishópa sem hún tilnefnir, skilgreinir hvaða hópar þetta eru, hvernig samstarfinu er háttað og hvaða gögnum skal skila til þeirra".*

Ennfremur er eftirfarandi ákvæði í 26. gr. í reglum Póst- og fjarskiptastofnunar nr. 1222/2007 um virkni almennra fjarskiptaneta, þar með talið almenna símkerfið;

✓ *„Í þeim tilgangi að auka heildstæði og öryggi fjarskiptaneta, getur Póst- og fjarskiptastofnun ákveðið að tiltekin gögn er varða öryggisatvik sem stofnað geta rekstri fjarskiptaneta í hættu, skulu afhent öryggishópi sem starfar samkvæmt 25. gr. reglna nr. 1223/2007 um vernd, virkni og gæði IP fjarskiptaþjónustu".*

Ennfremur segir í 24. grein í sömu reglum:

✓ *„Gögn um ósamfellda virkni og önnur öryggisatvik í mikilvægum innviðum fjarskiptaneta er varða þjóðaröryggi sérstaklega, skal senda til þeirra aðila sem hafa þar hlutverki að gegna. Póst- og fjarskiptastofnun skilgreinir nánar hvaða innviðir koma við sögu, hvaða aðilar þetta eru og hvaða gögnum skal skila til þeirra".*

6.4 TILMÆLI ESB UM STOFNUN/STYRKINGU FORYSTU CSIRT TEYMA

[8] Með öryggishópi er átt við CSIRT-teymi

ESB hefur oft bent aðildarþjóðunum á hversu mikilvæg CSIRT teymi eru, og sérstaklega það lykilhlutverk sem stjórnsýslu- eða þjóðar-CSIRT hafa til að stuðla að vernd gagnvart ógnum í innviðum Internetsins. Sömuleiðis er lögð áhersla á samvinnu þessara hópa innan Evrópu og á alþjóðlegum vettvangi. Stefna ESB nú er að þessi forystu-teymi útvíkki verksvið sitt og stuðli að vernd allra innviða í fjarskipta- og upplýsingatækni, þ.m.t. langlínu- og farsímaneta.

6.4.1 INTERNETIÐ Í BRENNIDEPLI TIL AÐ BYRJA MEÐ

Fyrsta stefnumörkunin kom fram í boðskiptum á árinu 2001 um „**Network and Information Security: Proposal for a European Policy Approach**“[9]. Þar kemur m.a. eftirfarandi fram í lauslegri þýðingu um Evrópskt viðvörunar- og upplýsingakerfi:

„Aðildarþjóðirnar ættu að styrkja sín CSIRT teymi og efla samhæfingu meðal þeirra. Framkvæmdastjórnin og aðildarþjóðirnar á Evrópusvæðinu munu í sameiningu kanna æskilega gagnaöflun um, greiningu á, og viðbrögð við núverandi og væntanlegum öryggisógnum“.

Í framhaldinu, þegar ENISA var stofnað 2004, var þetta haft að leiðarljósi, er stofnuninni voru úthlutuð meðal annars CSIRT málefni. - ENISA hefur síðan þá unnið ötullega að útbreiðslu CSIRT teyma innan Evrópu.

6.4.2 ÁHERSLA Á ALLA FJARSKIPTA- OG UPPLÝSINGAINNVIÐI Í DAG

Í byrjun næsta árs mun framkvæmdastjórnin leggja til stefnumótun um málefni mikilvægra fjarskipta- og upplýsingainnviða[10] sem gerir ráð fyrir uppsetningu varna sérhverrar aðildarþjóðanna gegn öryggisatvikum á grundvelli stjórnsýslu- eða þjóðar-CSIRT teyma sem hornsteinn[11]. Einn af lykilþáttum við vernd mikilvægra fjarskipta- og upplýsingainnviða er endurbætur á getu til að sporna við öryggisatvikum á alþjóðlega vísu og innan ESB. Hugmyndin er að óska eftir að aðildarþjóðirnar komi á/styrki þjóðarvarnir gegn öryggisatvikum. Þetta yrði líklega gert á vettvangi stjórnsýslu- eða þjóðar-CSIRT teyma sem lykilhlutverk í viðbúnaði, upplýsingamiðlun, samhæfingu og mótaðgerða gegn öryggisatvikum. Þungamiðjan í slíkri þjóðvarnagetu væri að koma á almannaæfingu í rekstrarsamfellu og viðreisn eftir stóráföll. Aðildarþjóðirnar mun ennfremur vera hvattar til að styrkja samevrópska samvinnu milli stjórnsýslu-/þjóðar-CSIRT teyma með það að markmiði að auðvelda upplýsingamiðlun, m.a. um tæknilegar ráðstafanir og bestu leiðir. Ennfremur auka viðbúnað með skipulögðum svæðisbundnum æfingum og/eða samevrópskum æfingum, þar sem líkt er eftir stóru öryggisatviki svo sem netárás, og auðvelda samskipti og samvinnu milli þjóðvarnaliða þegar upp koma alvarleg áföll og þjóðfélagslegar kreppur. Þjóðar- eða stjórnsýslu-CSIRT teymi geta gengt lykilhlutverki í þessu öllu.

Til þess að styðja við þetta markmið hefur framkvæmdastjórn ESB falið ENISA, í samvinnu við aðildarþjóðirnar, að vinna að verkefninu WPK2.2 – Security Competence circle and good practice sharing at the EU level“ sem hefur það markmið að styrkja frekari samvinnu og miðlun bestu leiða í CSIRT samfélögum innan ESB. Þ.e. að taka saman gögn um bestu leiðir, og gera leiðbeiningar er fjalla um þá grunnþjónustu og -verkefni sem nýtast kunna stjórnsýslu- eða þjóðar-CSIRT teymum sem verðandi

[9] COM(2001) 298 - „Net- og upplýsingaöryggi“

[10] CII – Critical Communication and Information Infrastructure – Mikilvægir innviðir í fjarskipta- og upplýsingatækni, þ.e. Internetið og aðrir innviðir fjarskipta.

[11] Skv. heimildum sem Póst- og fjarskiptastofnun hefur fengið frá lykilaðila innan ESB

máttarstólpa í þjóðvörnum aðildarríkjanna gegn áföllum í innviðum þeirra er varða þjóðaröryggi, sem og í skipulagðri og áhrifaríkri Evrópu-/alþjóðasamvinnu.

Af þessu má sjá að ESB lítur beinlínis á þjóðar-/stjórnsýslu-CSIRT teymi sem hornstein í vernd mikilvægra fjarskipta- og upplýsingainnviða í nánustu framtíð.

7 VERND MIKILVÆGRA INNVIÐA Í FJARSKIPTA- OG UPPLÝSINGATÆKNI[12]

ÁÐUR EN LENGRA ER HALDIÐ, ER RÉTT AÐ FJALLA UM HVERNIG MIKILVÆGIR INNVIÐIR Í FJARSKIPTA- OG UPPLÝSINGATÆKNI ER VARÐA ÞJÓÐARÖRYGGI GETA FALLIÐ AÐ STARFSEMI FORYSTU-CSIRT TEYMA.

7.1 INTERNETIÐ

Sammerkt með öllum CSIRT er að vinna að öryggismálum Internetsins. Bandaríkin skilgreina Internetið sem einn hinna mikilvægu innviða sinna í fjarskipta- og upplýsingatækni er varðar þjóðaröryggi. Sama á við mörg önnur lönd, svo sem Svíþjóð.

7.2 FJARSKIPTAGEIRINN

Nokkur forystu-CSIRT hafa einnig á sinni könnu mál er snerta aðra mikilvæga innviði fjarskipta-og upplýsingatækni er varða þjóðaröryggi í fjarskiptageiranum, t.d. CERT-FI í Finnlandi, m.a. í þeim tilgangi að styrkja röskunarþol innviðanna gegn öryggisatvikum. Þetta táknar að þau sinna líka öryggisatvikum í öðrum fjarskiptanetum en Internetinu, svo sem almennum símnetum og farsímanetum sem gætu talist til mikilvægra innviða fjarskiptageirans er varða þjóðaröryggi[13].

Hið sama gildir þegar aðrir geirar nýta sér almenn fjarskipta- og upplýsingakerfi, þ.e. aðilar svo sem fjármála og orkufyrirtæki eiga þess kost á að gerast hagsmunaaðilar. Ekki er um það að ræða að veita þeim vernd í sérhæfðum lokuðum netkerfum svo sem stýringum raforkukerfisins. Dæmi um aðstoð er að viðvaranir og ábendingar yrðu sendar viðkomandi hagsmunaaðilum, auk þess sem teymið tæki þátt í sameiginlegum varnaraðgerðum auk fyrirbyggjandi ráðstöfunum allra geira.

7.3 STEFNA ESB UM AUKIÐ RÖSKUNARÞOL INNVIÐA Í EVRÓPU

ESB leggur sífellt meiri áherslu á vernd mikilvægra innviða í fjarskipta- og upplýsingatækni með auknum viðbúnaði og getu til að mæta öryggisatvikum innan ESB svæðisins, svo sem netglæpum og nethryðjuverkum. Helstu fyrirséðu verkefni ESB eru þessi:

- Þróun á mælikvarða við að greina mikilvæga innviði fjarskipta í Evrópu.
- Aukin geta Evrópu í heild sinni til að mæta öryggisatvikum.
- Þróun á sterku og traustu samstarfi milli stjórnsýslunnar og einkaaðila við að útdeila innbyrðis hagnýtum upplýsingum og bestu leiðum.
- Styrking á alþjóðlegri samvinnu um landamæralaus málefni mikilvægra innviða fjarskipta- og upplýsingatækni, sérstaklega í auknu öryggi og áreiðanleika Internetsins.

[12] CIIP – Critical Communication and Information Infrastructure Protection – Vernd mikilvægra innviða í fjarskipta- og upplýsingatækni

[13] "Greining mikilvægra innviða í fjarskiptageiranum er varða þjóðaröryggi" er eitt verkefna PFS sem verður unnið að á árinu 2008.

Verkefni þessi eru mikilvægt skref ESB til innleiðingar á stefnu framkvæmdastjórnarinnar um „Secure Information Society“[14]

[14] COM(2006) 251 – „Öruggt upplýsingasamfélag“ - dags. 31.05.2006

8 FORYSTU-CSIRT ÚTFÆRSLA ÁKVEÐIN

8.1 STARFSSVIÐ AFMARKAÐ[15]

Almennt leitast CSIRT um allan heim við að notaðir séu sífellt betri innviðir neta og betri gangverk, sem annars vegar stuðla að traustari fjarskiptaleiðum og auknu röskunarþoli fjarskipta- og upplýsinganeta gegn netárásum, truflunum og bilunum, og skjótari samhæfingu viðvarana og viðbragða í neyð hins vegar. Í þessum tilgangi, þ.m.t. að viðhalda mikilvægri þjónustu á Internetinu óskertri og eignum ólöskuðum eftir netárásir, telja þau rétt að hugsanleg aukageta til styrkingar innviða sé nýtt skynsamlega, svo sem varaleiðir og tvítengingar. CSIRT vilja stuðla jafnt að auknu öryggi í nýgangsettum kerfum og hugbúnaði, auk betri flutnings- og aðgangsstýringum (þ.m.t. víðtæka innleiðingu á auðkenningu notenda). Forsenda fyrir framansögðu er að samtímis séu viðhafðar víðtækar ráðstafanir sem auðvelda beitingu aðgerða til upplýsingaöryggis og stjórnun þess.

CSIRT stuðla jafnframt að þjálfun og menntun í þeim tilgangi að auka tæknilega færni og þekkingu eigin starfsmanna og hagsmunaaðila sinna, s.s. í fjarskiptageiranum og annarra sem sjá um netöryggi.

Það sem hér hefur verið nefnt, er æskilegt að ræða og taka ákvarðanir um á breiðari grundvelli. Ekki aðeins innan einstakra fyrirtækja og samsteypa, heldur á landvísu undir forystu þess teymis sem jafnframt starfar á alþjóðlega vísu. Slíkt fyrirkomulag eykur skilvirkni við að stytta tímann sem mest frá því ný ógn kemur fyrst í ljós, hún er greind og brugðist við henni. Á þennan hátt yrðum við fyrir minna tjóni og kostnaður lækkar við að koma hlutunum í samt lag.

Í veröldinni eru tiltölulega fá fyrirtæki og stofnanir með CSIRT innan sinna vébanda, eða áætlun um stjórnun upplýsingaöryggis, og oft skortir alfarið ferla til að fást við öryggisatvik. Einnig skortir nokkrar þjóðir varnir gegn öryggisatvikum á landsvísu, svo og stjórnunar- og samhæfingarferla. Hliðstætt við CSIRT-lausu fyrirtækin eru þessar þjóðir í meiri hættu en aðrar sem eru betur útbúnar. Nokkur þessara landa ráða hvorki yfir stuðningsnetkerfum, hæfum starfsmönnum né búnaði til að vakta ógnandi virkni á áhrifaríkan hátt og vernda mikilvæga þjónustu. Þær bregðast ekki skipulega við alvarlegum atvikum sem koma upp í net- og tölvukerfum mismunandi þjónustugeira í hverju landi, t.d. í fjármálageiranum, heilsugeiranum o.s.frv. Í hnotskurn má segja að skilningsskortur á undirliggjandi öryggisþáttum og á mikilvægi samhæfingar, opni fleiri glufur fyrir þrjóta sem þeir nýta sér til að komast yfir viðkvæm gögn almennings þessara landa. Þetta þýðir að fjármunir tapast frekar og önnur skakkaföll ríða yfir.

Í ljósi frumkvæðis stjórnvalda við fyrirhugaða stofnun CSIRT, er myndi bregðast við hvers konar vá sem stafar að íslenskum netkerfum, og hlutverks Póst- og fjarskiptastofnunar í því verkefni, gerum við ráð fyrir að hér séum við að undirbúa stofnun þess teymis sem mun verða í forystuhlutverki gegn öryggisatvikum í

[15] Stuðst við gögn frá CERT/CC

fjarskiptatengdri upplýsingatækni á Íslandi. Teymið hefði jafnframt forystu fyrir flestum öðrum CSIRT teymum sem kunna að koma í kjölfarið hér á landi.

Í útlöndum er yfirleitt eitt slíkt forystu-CSIRT í hverju landi, í einni eða annarri mynd. Hlutverk þeirra er oftast sameiginlegur vettvangur samskipta gegnum samstarfsnet um öryggisatvik innanlands og við útlönd. Ennfremur stuðningur við vernd netkerfa í viðkomandi landi. Þessi atriði koma skýrt fram í áðurnefndum hugmyndum stjórnvalda hér á landi í tengslum við fyrirhugað CSIRT teymi.

Að teknu tilliti til alvarleika þeirrar hættu sem vofir yfir íslenskum netkerfum og yfirlýsingum stjórnvalda um málefni CSIRT, auk þeirrar stefnu ESB að að forystu-CSIRT eigi að sinna öllum almennum fjarskipta- og upplýsinganetum, má því ganga að því sem vísu að helsta afmarkaða starfssvið teymisins yrði a.m.k. eftirfarandi:

- *Samhæfa aðgerðir um vernd upplýsinga í íslenskum fjarskipta- og upplýsinganetum, gegn öryggisatvikum eins og kostur er*. Hér er m.a. átt við samhæfingarmiðstöð viðvörunar og viðbragða gegn netvá á landsvísu sem er eitt aðalhlutverka þjóðar-CSIRT teyma.
- *Rekstur samskiptamiðstöðvar (PoC – Point of Contact) í tengslaneti innanlands, og við önnur lönd um mál sem snerta öryggisatvik í fjarskipta- og upplýsingatækni.* Almennt er þetta jafnframt eitt aðalhlutverk þjóðar-CSIRT teyma. Opinber stofnun, t.d. eftirlitsstofnun svo sem Póst- og fjarskiptastofnun getur líka tekið þetta að sér. Ennfremur kemur til greina að stjórnsýslu-CSIRT sinni þessu hlutverki, þótt aðalstarfsemi þess myndi afmarkast að mestu við vernd net- og upplýsingakerfa stjórnsýslunnar.

Þess má geta að mat skýrsluhöfundar er að starfssvið WARP viðvörunarhópa, sem fjallað er um í viðauka E, er það þröngt að þeir henti ekki ofangreindu hlutverki.

8.2 ÚTFÆRSLA CSIRT FORYSTUTEYMIS

Eins og lýst er í viðauka A um "Ýmsar CSIRT útfærslur" eru til nokkrar tegundir slíkra teyma sem hafa mismunandi ábyrgð, fjármögnun, hagsmunaaðila o.s.frv. Meðal þeirra eru tvær gerðir CSIRT sem koma til greina miðað við það starfsvið sem fyrr kom fram; annars vegar stjórnsýslu-CSIRT og hins vegar þjóðar-CSIRT.

Stjórnsýslu-CSIRT leggur megináherslu á öryggi eigin netkerfa og tilheyrandi tölvukerfa innan stjórnsýslunnar og ráðleggingar sem tengjast þeim. Hagsmunaaðilar slíks teymis eru fyrst og fremst stjórnsýslan en dæmi eru um að slík teymi útvíkki starfsemi sína í átt að starfsemi þjóðar-CSIRT.

Þjóðar-CSIRT starfrækir hins vegar samstarfsnet innan íslenskrar netþjónustu. Ólíkt stjórnsýslunnar-CSIRT er þetta teymi ekki með höfuðáherslu á hið opinbera. Aðaláherslan er í þessu tilfelli lögð á vernd almennra íslenskra fjarskipta- og upplýsinganeta gegn hvers konar öryggisatvikum. Ennfremur rekstur fyrrgreinds samstarfsnets milli aðila. Samskipti teymisins eru að mestu bundin við áhrifasvæði þess, en innan þess eru þeir sem veita fyrrgreinda þjónustu og gera þjónustusamning við þjóðar-CSIRT teymið þar að lútandi.

Hér á eftir er lausleg upptalning á mögulegri starfsemi og áhrifasvæði þessara tveggja leiða, staðfært á íslenskt umhverfi:

- Íslenskur þjóðar-CSIRT
    - Stuðlar að vernd almennra þjóðarneta á Íslandi í fjarskipta- og upplýsingatækni (áhrifasvæði teymisins).
    - Er í forsvari samtaka íslenskra CSIRT teyma sem kunna að koma í kjölfarið.
    - Sérhvert CSIRT teymi innan samtakanna er ábyrgt gagnvart hagsmunaaðilum sínum. Venjulega er samvinna höfð milli mismunandi hagsmunaaðila, í þeim tilgangi að safna saman gögnum til úrvinnslu sem eru nauðsynleg fyrir rannsóknarvinnu. Þjóðar-CSIRT heldur utan um þessa samvinnu þannig að upplýsingar og gögn myndi eina heild. Meðal verksviða teymisins gæti verið eftirfarandi:
        - Stuðla að samhæfðri vernd gegn öryggisatvikum er upp kunna að koma og bregðast snöggt við.
        - Starfræksla samskiptamiðstöðvar í samstarfsneti innan samtakanna og við útlönd.
        - Veita fjölmiðlun upplýsingar um almennt net- og tölvuöryggi.

- Stjórnsýslu-CSIRT á Íslandi
    - Stuðlar að vernd í nettengdum upplýsingakerfum hins opinbera (áhrifasvæði teymisins).
    - Aðal verksviðið er starfræksla miðlægrar stjórnstöðvar er stuðlar að forvarnar- og viðbragðs ráðstöfunum gegn öryggisrofi, hugsanlegri þjónustusynjun og gegn öðrum öryggisatvikum í net- og tölvukerfum hins opinbera sem er áhrifasvæði teymisins. Þetta er m.a. gert með viðvörunar- og upplýsingaþjónustu og greiningu atvikatilkynninga, auk útgáfu ráðlegginga í framhaldinu. Eftirfarandi verkefni koma því til greina:
        - Rekstur á virku viðvörunarkerfi fyrir stjórnvöld í áríðandi neyðartilfellum, með allt að 24 stunda síma- og viðvörunarvakt.
        - Veita stjórnvöldum ráð um almennt net- og tölvuöryggi.
        - Semja og birta ráðleggingar til rekstrarstjóra netkerfa stjórnsýslunnar um fyrirbyggjandi ráðstafanir í þeim tilgangi að hindra skaða, m.a.:
            - Ábendingar um veikleika í vél- og hugbúnaði.

- Ábendingar og ráðleggingar um að komið verði í veg fyrir þekkta öryggisveikleika.
- Vara við alvarlegum ógnum sem beint er að upplýsingatækni.
- Mæla með viðbrögðum sem takmarka tjón eða eyðingu.

Mismunur á þessum tveimur lausnum á samsetningu CSIRT liggur sem sagt í áherslumun, þar sem annars vegar er stjórnsýslan í miðpunkti og hins vegar landið allt. Starfsemi beggja leiða er álíka umfangsmikil og sum lönd reka hvort tveggja. Stundum er áhrifasvæði annars þeirra stækkað inn á áhrifasvæði hins, t.d. ef stjórnsýslu-CSIRT sinnir líka almennum þjóðarnetum að hluta.

Við teljum þjóðar-CSIRT henta betur, þar sem það er algengara og fellur betur að þeim forsendum sem fjallað er um hér að framan. Meðan ekki eru önnur CSIRT teymi innan vébanda þess, færast aðrir hagsmunaaðilar upp í forgangi.

9 VERKSVIÐ ÞJÓÐAR-CSIRT TEYMA

9.1 ALGENGT VERKSVIÐ ÞJÓÐAR-CSIRT TEYMA[16]

Verksvið flestra þjóðar-CSIRT teyma er frekar víðtækt, þó það sé ekki alls staðar eins. Grunn starfsemin er þó svipuð frá einu landi til annars en breytileg áhersla er lögð á nokkra aðra þætti starfseminnar. Eins og áður var greint frá vinna þjóðar-CSIRT á landsvísu. Þ.e., tilgangur þeirra í sinni víðtækustu mynd er *„að stuðla að vernd mikilvægra innviða og annarra lykilþátta fjarskipta- og upplýsinganeta innan netlögsögu viðkomandi lands, auk þess að koma á og viðhalda samstarfsneti við önnur CSIRT“.*

Við skulum byrja á að greina betur flesta þá þætti sem koma til greina í starfsemi þjóðar-CSIRT teyma, þar sem fjöldi stjarna táknar lauslega áætlað mikilvægi:

- (****) Reka samhæfingarmiðstöð (Cooperational Center) meðal hagsmunaaðila til höfuðs öryggisatvikum á Íslandi eða innan netlögsögu Íslands, með samstilltu átaki og beinni samvinnu um meðhöndlun öryggisatvika. Þ.e.a.s. samhæfingarmiðstöð viðvörunar og viðbragða gegn netvá á landsvísu sem er eitt aðalhlutverka þjóðar-CSIRT. Ennfremur er æskilegt að slík vinna beinist gegn hugsanlegum atvikum og ógnum sem stofnað geta mikilvægum innviðum í hættu er varða þjóðaröryggi. Samhæfingarmiðstöð þarf að vera vakandi yfir, og geta beint starfi sínu gegn, þeirri þróun sem netárásir virðast stefna í á hverjum tíma.

- (****) Starfrækja samskiptamiðstöð (PoC – Point of Contact) í tengslaneti innanlands, og við önnur lönd um mál sem snerta öryggisatvik í almennum fjarskipta- og upplýsinganetum. Samstarfsnetið er rekið á traustu gangverki samskipta sem hagsmunaaðilar geta treyst, þ.e.a.s. nokkurs konar gáfum gætt skiptiborð sem kemur á og miðlar samskiptum milli hagsmunaaðila um málefni öryggisatvika. Auk þess tekur samskiptamiðstöðin við tilkynningum um öryggisatvik þegar sendandinn (t.d útlent CSIRT teymi) veit ekki hvert á að tilkynna þau. Í þeim tilvikum áframsendir teymið beiðnina til réttra aðila, eða veitir sjálft lágmarks aðstoð. Hér er mjög mikilvægt að það sé fyllilega ljóst hvaða CSIRT teymi er skilgreint sem samskiptamiðstöð til að taka við slíkum fyrirspurnum. Í nokkrum löndum er þetta ekki nógu ljóst og rýrir það tiltrú á starfssemi þeirra.

- (****) Þjóðar-CSIRT hefur ekki beint skipunarvald yfir hagsmunaaðilum sínum, heldur byggist starfsemin upp á samvinnu og áunnu trausti milli aðila.

- (***) Styðja við skráningu öryggisatvika innanlands meðal ólíkra sviða samfélagsins, svo sem innan stjórnsýslunnar, verslunar, háskóla, banka og fjármálastofnana o.fl.

- (***) Leiða atvika-, veikleika- og búnaðargreiningu, ásamt því að dreifa gögnum um atvik og berskjölduð tölvu- og fjarskiptakerfi. Gögnin berast m.a. frá öðrum CSIRT teymum, framleiðendum og sérfræðingum um UT-tækni, í þeim tilgangi að meta hugsanleg áhrif þeirra innan eigin áhrifasvæðis. Ennfremur gefa hagsmunaaðilum, samstarfsaðilum, hlutaðeigandi, og öðrum aðilum sem njóta trausts teymisins viðhlítandi ráð sem draga úr áhrifum atvikanna.

[16] Stuðst við gögn frá CERT/CC

- (***) Aðstoða hagsmunaaðila sína við að auka eigin færni í að stjórna meðhöndlun öryggisatvika. Jafnframt að gefa fyrirtækjum og stofnunum ráð og upplýsingar vegna undirbúnings og stofnunar nýrra CSIRT, auk þess að mynda tengsl og efla umræður meðal hlutaðeigandi aðila. Þeir geta líka metið árangur annarra CSIRT teyma innanlands og borið ábyrgð á vottun/viðurkenningu þeirra.

- (***) Styðja við, eða taka þátt í áætlun um námsþjálfun, vitundarvakningu og þjálfunarefni sem hentar hinum ýmsu hópum þjóðfélagsins, svo sem kerfis- og netstjórum, öðrum innlendum CSIRT teymum, stjórnendum, lögmönnum, framkvæmdavaldi, eftirlitsstofnunum eða hinum almenna netnotanda.

- (***) Að auki getur íslenskt þjóðar-CSIRT samstillt strengi sína með öðrum útlendum þjóðar-CSIRT með því að leggja til sérfræðinga sína á vogarskál aukins skilnings á öryggisatvikum og berskjölduðum kerfum.

- (***) Örfá þjóðar-CSIRT hafa jafnframt hafið þátttöku í nýju alþjóðlegu "vöktunar- og aðvörunar" samstarfsátaki til að auka öryggi á Internetinu. Hefur ESB töluverðan áhuga á þessu samstarfsverkefni.

- (***) Taka þátt í alþjóðlegu samstarfi um öryggi Internetsins, sem eflir og styður við teymi frá mismunandi löndum sem deila með sér töluupplýsingum, rannsóknarupplýsingum, varnarstefnu og aðvörunum hvers annars. Þátttakendur dreifa þessum upplýsingum í gegnum sérstaka mikilvæga innviði sína, sem teygja sig milli landa.

- (***) Þjóðar-CSIRT getur líka myndað tengsl við yfirvöld um málefni sem lúta að mikilvægum innviðum og þjóðaröryggi í víðum skilningi, þ.e. í þeim tilfellum þar sem ekki eru sérhæfðari CSIRT sem sinna því.

- (**) Þýða efni um öryggismál yfir á íslensku, t.d. rannsóknir á spilliforritum o.fl.

- (**) Veita aðgengilegar upplýsingar og ráð um öryggismál, t.d. á vefsíðu, með útgáfustarfsemi eða með öðrum hætti. Slíkar upplýsingar gætu innihaldið gögn um neta- og vélastillingar, vefslóðir um gagnlegt efni um örugg netsamskipti, eða annað sem hjálpar notendum að auka öryggi í heimilistölvum.

- (**) Viðhalda skráningu á verksviði og færni annarra innlendra CSIRT teyma, ásamt tengiliðum.

- (**) Þjóðar-CSIRT sumra landa aðstoða löggjafarvaldið og stjórnvöld með tækniþekkingu sinni, þótt það sé ekki hluti af fyrrgreindri kjarnastarfsemi þeirra. Ákjósanlegt er að mynda samskiptatengsl milli þessara aðila um net- og tölvuöryggi, svo sem í þeim tilgangi að auðvelda samræmingu í öllu þjóðfélaginu við stórum áföllum.

- (*) Í nokkrum löndum hafa stjórnvöld ályktað sem svo, að það sé hlutverk þjóðar-CSIRT teymisins að framkvæma aðgerðir í búnaði til að bregðast við alvarlegum öryggisatvikum á Internetinu. Þ.e.a.s. fara á staðinn og slökkva elda, í stað þess að vera ráðgefandi og leiðandi í þeim efnum. Sumar opinberar stofnanir hafa sett ákvæði í reglur sem beinlínis skylda teymið til að sinna þeim þætti, auk annarra skyldustarfa s.s. að gefa út ársskýrslu um öryggismál.

<u>Það sem er merkt með þremur og fjórum stjörnum má segja að sé grunnstarfsemi flestra þjóðar-CSIRT teyma.</u>

10 ÍSLENSKT ÞJÓÐAR-CSIRT – LÝSING Á STARFSEMI OG ÁVINNINGUR

VIÐ STOFNUN ALLRA CSIRT TEYMA ER MIKILVÆGT AÐ VERKEFNIÐ SÉ SKÝRT SKILGREINT FRÁ UPPHAFI. HÉR VERÐUR LÝST MÖGULEGRI STARFSEMI ÍSLENSKS ÞJÓÐAR-CSIRT TEYMIS.

10.1 VERKSVIÐ

Í víðum skilningi er verksvið þjóðar-CSIRT teyma að leiða rannsókn og meðhöndlun á öryggisatvikum í nettengdri upplýsingatækni á landsvísu.

Að teknu tilliti til íslenskra aðstæðna og minni fjárhagsramma en stærri þjóðir hafa til umráða, gætum við þurft að sætta okkur við þrengra starfssvið en helstu nágrannalönd okkar. Til þess að starfsemi íslenska þjóðar-CSIRT teymisins nálgist hugmyndir stjórnvalda, þarf að lágmarki það sem merkt er með fjórum stjörnum í kaflanum hér á undan að fylgja starfseminni, , þ.e. samhæfingar- og samskiptamiðstöð auk viðvörunarþjónustu. Og traust þarf alltaf að vera til staðar sem góður grunnur að öllum samskiptum.

Best virkar teymið ef sú starfsemi sem merkt er með þremur stjörnum er ákveðin líka. Íslenska teymið yrði þá vettvangur samskipta innanlands og utan og samhæfði meðhöndlun öryggisatvika. Að auki vaktaði teymið tilfallandi öryggisatvik innan netlögsögu Íslands, skráði niður viðburði og útbyggi tölfræðiskýrslur. Ennfremur myndi það aðvara hagsmunaaðila sína gagnvart yfirvofandi hættum og uppfræðaog ráðleggja þeim um varnarráðstafanir og fyrirbyggjandi aðgerðir.

Gert er ráð fyrir að starfsemin miðist við vernd mikilvægra innviða fjarskipta- og upplýsinganeta er varða þjóðaröryggi, skv. stefnu ESB. Það fellur ágætlega undir starfssvið þjóðar-CSIRT teyma.

Svikastarfssemi tengist ekki öryggisatvikum nema viðkomandi þrjótur hafi beinlínis fært sér í nyt innbrot í berskjölduð upplýsingakerfi, netárásir, spilliforrit eða önnur öryggisatvik við verknaðinn. Að því leyti sem snýr að því að koma í veg fyrir frekari útbreiðslu slíkra öryggisatvika, er hugsanlegt að þjóðar-CSIRT hafi samstarf við lögregluyfirvöld við lausn þessara mála og samræmingu aðgerða. Sú staða gæti komið upp að vinna við tiltekið mál væri samstarfsverkefni þjóðar-CSIRT, Póst- og fjarskiptastofnunar, fjarskiptafyrirtækja og lögregluyfirvalda.

10.2 ÁHRIFASVÆÐIÐ SKILGREINT

Þjóðar-CSIRT teymi stuðla fyrst og fremst að vernd á áhrifasvæði sínu gegn öryggisatvikum, þ.e. viðkomandi þjóðar í heild sinni.

Í ljósi fyrrgreinds hlutverks CSIRT á landsvísu, og þeirrar staðreyndar að nettengdar tölvur spjalla við aðrar nettengdar tölvur, þ.e. IP vistföng, og öryggisatvik má rekja beint til slíkra vistfanga en sjaldnast til einstaklinga, er hentugt að binda áhrifasvæðið við þau. Þar sem Internetið teygir sig til allra landa þarf okkar þjóðar-CISRT teymi líka að stuðla að vernd þess í heild sinni. En íslensk netkerfi eru í fyrsta forgangi og má því slá því föstu að áhrifasvæði þjóðar-CSIRT teymisins sé eftirfarandi (í forgangsröð):

- Íslensk netkerfi og netþjónusta sem veitt er gegnum íslensk AS-númer - Þ.e. innan netlögsögu Íslands og gildir einu hvort starfsemi viðkomandi notenda er alfarið á Íslandi eða að hluta gegnum starfsstöðvar í útlöndum.

- Önnur IP netkerfi og netþjónusta á heimsvísu

- Aðrir mikilvægir innviðir fjarskipta- og upplýsinganeta og tengd þjónusta

10.3 HAGSMUNAAÐILAR SKILGREINDIR

Breytilegt er milli landa hvernig hagsmunaaðilar þjóðar-CSIRT eru skilgreindir. Við höfum kosið að binda skilgreininguna við þá aðila sem veita fjarskipta- og fjarskiptaöryggisþjónustu til viðskiptavina sinna. Þeir eru eftirfarandi í forgangsröð:

- Íslensk CSIRT teymi sem gert er samkomulag við um að vera hagsmunaaðili.
- Aðrir aðilar sem gert er samkomulag við, t.d. netöryggisdeildir stórra fjarskiptafyrirtækja og hins opinbera, orku- og bankageirinn o.s.frv.
- Önnur ósamningsbundin CSIRT teymi á Íslandi, með sérstaka áherslu á aðstoð við ný CSIRT sem er verið að stofna
- CSIRT teymi í Evrópu
- Önnur útlend CSIRT teymi

Fremstu hagsmunaaðilar eru því önnur íslensk CSIRT, t.d. innan raða íslenskra fjarskiptafyrirtækja, hins opinbera eða CSIRT sem tilheyra tilteknum geira, svo sem orku- eða bankageiranum. Þar á eftir koma netöryggisdeildir þeirra aðila sem ekki hafa formlegan CSIRT innan sinna vébanda, svo sem fjarskiptafyrirtækja, stærri fyrirtækja og opinbera stofnana.

10.4 VIÐSKIPTAVINIR HAGSMUNAAÐILANNA

Notendur íslenskra netkerfa og netþjónustu, t.d. þorri íslensks almennings eru viðskiptavinir hagsmunaaðilanna. Sama gildir um viðskiptavini tiltekins banka sem hefur gert samning um skjólstæði. Við þá hefur þjóðar-CSIRT teymið lítil eða engin samskipti, enda þarf starfsemin þá að vera mun viðameiri. Vissulega verður tekið við ábendingum frá almenningi og viðskiptavinum, en þeim verður ekki veitt bein aðstoð við vandamál er upp kunna að koma í tölvu viðkomandi. Eins og áður sagði njóta viðskiptavinirnir þó alltaf óbeint þess öryggis sem starfsemi þjóðar-CSIRT leiðir af sér.

10.5 ÁVINNINGUR VIÐ REKSTUR ÞJÓÐAR-CSIRT TEYMIS Á ÍSLANDI

Íslenskt þjóðar-CSIRT stuðlar að sem minnstum áhrifum öryggisatvika, t.d. með vernd gegn öryggisatvikum í íslenskum netkerfum og netþjónustu sem standa almenningi til boða, til hagsbóta fyrir alla landsmenn.

Teymið er í viðbragðsstöðu gagnvart alvarlegum öryggisatvikum og öðrum áföllum í fjarskiptatengdri tölvutækni. Teymið gefur hagsmunaaðilum sínum viðvaranir þegar við á, gefur ráðleggingar og samhæfir varnaraðgerðir þegar þess er þörf.

Algeng verkefni íslensks þjóðar-CSIRT teymis verða eftirfarandi:

- Hagsmunaaðilar leita til þjóðar-CSIRT teymisins sem miðpunkts samhæfingar og viðvarana gegn öryggisatvikum í fjarskipta- og upplýsinganetum sínum.
- Teymið leggur sérstaka áherslu á vernd mikilvægra innviða í fjarskipta- og upplýsinganetum.
- Teymið bregst kerfisbundið við slíkum öryggisatvikum og grípur til viðeigandi ráðstafana.
- Teymið aðstoðar hagsmunaaðila sína á skjótan og árangursríkan hátt við að koma hlutunum í samt lag eftir að öryggisatvik hefur komið upp og heldur tjóni vegna þjófnaðar á upplýsingum eða rofi á þjónustu í lágmarki.
- Teymið hagnýtir sér þær upplýsingar sem safnast við hvert öryggisrof til að stuðla að betri vörnum fyrir tölvukerfi og vernd upplýsinga.
- Þjóðar-CSIRT teymið bregst á réttan hátt við þegar lagaleg atriði koma upp í tengslum við öryggisatvik.
- Það leggur áherslu á að hagsmunaaðilarnir deili með sér þekkingu um öryggismál.
- Það leitast við að styrkja ímynd hagsmunaaðilanna í tæknilegu og markaðslegu tilliti.

Dæmi um ávinning af rekstri þjóðar-CSIRT teymisins[17]:

- Þung netatlaga kemur að utan sem er beint að heimabanka fjármálastofnunar. Atlagan kemur í gegnum fjarskiptanet tveggja íslenskra fjarskiptafélaga. Þjóðar-CSIRT teymið er í beinu sambandi við og samhæfir varnaraðgerðir hlutaðeigandi aðila, þ.e. bankans, fjarskiptafélaganna og þjóðar-CSIRT þess lands sem atlagan er gerð frá. Tími og fjármunir sparast vegna markvissrar varnar og orðspor bankans og fjarskiptafélaganna bíður síður hnekki.
- Gegnum Internetið er stolið persónuupplýsingum hóps Íslendinga frá íslenskri heilbrigðisstofnun. Þessar upplýsingar eru birtar á ákveðinni vefsíðu í útlöndum. Þjóðar-CSIRT teymið vinnur með hlutaðeigandi, þ.m.t. þjóðar-CSIRT teymi þess lands þar sem upplýsingarnar eru birtar, til þess að reyna að loka fyrir frekari birtingu upplýsinganna. Óþægindi þau sem viðkomandi einstaklingar verða fyrir eru í lágmarki með markvissum aðgerðum og ef vel tekst til.
- Dulkóðun er brotin í SMS samskiptum á Íslandi á þann hátt að óheimil hlerun á sér stað víða. Þjóðar-CSIRT teymið veitir ráð og vinnur með hlutaðeigandi aðilum um samstíga lausn vandamálsins. Almenningur er upplýstur um þróun mála og treystir frekar þessum samskiptamáta á ný eftir markvissar aðgerðir.
- Öflugur jarðskjálfti verður nálægt Heklu sem rýfur fjarskiptasambönd við farsímasenda, við virkjanir og endurvarp útvarps og sjónvarps. Þjóðar-CSIRT teymið greinir ástandið og setur sig í beint samband við, og samhæfir aðgerðir í fjarskipta- og upplýsinganetum, hluteigandi orku- og fjarskiptafyrirtækja, svo og fjölmiðla. CSIRT teymið stuðlar þannig að sneggri endurreisn neta og kerfa og að upplýsingaboð berist íbúum svæðisins sem skjótast.

Eins og fyrr er getið getur fjárhagslegur ávinningur verið töluverður fyrir hvert prósentustig sem forystu-CSIRT stuðlar að minnkandi áhrifum öryggisatvika.

[17] Þjóðar-CSIRT fer ekki inn á svið lögregluyfirvalda en samráð getur verið milli þeirra

10.6 TRAUST ER GRUNDVÖLLUR STARFSEMINNAR

Ef rekstur þjóðar-CSIRT teymis á að ganga vel fyrir sig þarf undirliggjandi traust milli hluteigandi aðila að vera sterkt. Byggja verður því upp traust strax með eftirfarandi kröfum:

- Hagsmunaaðilarnir þurfa að geta treyst þjóðar-CSIRT sem óháðum aðila og deilt upplýsingum með honum.
- Mikilvægt er að þjóðar-CSIRT njóti trausts innan net-, tölvu- og fjarskiptamarkaðarins.
- Kynna þarf hagsmunaaðilum vel starfsemina.
- Mynda þarf góð tengsl við almenn CSIRT teymi á alþjóðlega vísu.
- Veita þarf skjóta og vandaða þjónustu.

10.7 HÖFUÐ- OG UNDIRMARKMIÐ[18]

Í ljósi fyrri umfjöllunar ættu höfuð- og undirmarkmið þjóðar-CSIRT að vera:

- Að koma í veg fyrir öryggisatvik á árangursríkan hátt, t.d. með því að:
    - Safna upplýsingum.
    - Miðla upplýsingum.
    - Miðla þekkingu.
    - Safna sérfræðiþekkingu.
    - Fá mismunandi aðila til samstarfs og samræðna til að deila upplýsingum.
    - Aðstoða önnur CSIRT í samfélaginu.
    - Fylgjast með þróun og framvindu og greina áhættu.
    - Skipuleggja sjálfsnám.
- Bregðast við öryggisatvikum á árangursríkan hátt, t.d með því að:
    - Skipuleggja og samhæfa viðbrögð við öryggisatvikum.
    - Nota rétt verkfæri og verkferla.
    - Að kynna sér sitt eigið áhrifasvæði með reglulegum spurningum um tækni og skipulag. starfsemi hagsmunaaðilanna.
    - Viðhafa virkt öryggiseftirlit.
- Vera miðpunktur samskipta um öryggisatvik innanlands og við útlönd, t.d með því að:
    - Koma á sameiginlegum vinnufundum með öðrum hugsanlegum CSIRT teymum innanlands.
    - Stuðla að mótun sameiginlegrar stefnu þeirra um samvinnu gegn öryggisatvikum í íslenskum fjarskipta- og upplýsinganetkerfum og birta opinberlega.
    - Stuðla að gerð verklagsreglna um samskipti meðal íslenskra CSIRT teyma og birta opinberlega.
    - Virka sem miðpunktur samskipta um öryggisatvik við útlönd og innanlands.
- Vara hagsmunaaðilana við öryggisatvikum, t.d með því að:

[18] Stuðst við gögn frá GovCERT í Hollandi

- Birta mikilvægustu erlendu viðvaranirnar um öryggisatvik, veikleika í kerfum o.fl. á opinni heimasíðu sinni og póstlistum.
- Birta sömuleiðis eigin viðvaranir, og hvað ber hæst á hverjum tíma, ef svo ber undir.

10.8 LEIÐARLJÓS STARFSEMINNAR

Tilgangur starfseminnar er að styðja við og styrkja upplýsingaöryggi innan íslenskra netkerfa. Þetta má taka saman í eftirfarandi leiðarljós:

"Þjóðar-CSIRT teymið veitir upplýsingar og aðstoð við að verja íslensk fjarskipta- og upplýsinganet, og tengda þjónustu, sem eru þjóðfélaginu mikilvæg. Teymið bregst við og samhæfir aðgerðir og gerir aðrar ráðstafanir til að minnka eða koma í veg fyrir áhrif alvarlegra öryggisatvika í mikilvægum innviðum hagsmunaaðila sinna á sviði fjarskipta- og upplýsingatækni".

Teymið þarf að hafa eftirfarandi hugfast:

- ✓ Við framkvæmum það sem við lofum.
- ✓ Við leggjum áherslu á fyrirbyggjandi aðgerðir gegn netvá og bjóðum upp á lausnir.

10.9 NAFN ÞJÓÐAR-CSIRT TEYMISINS

CSIRT teymi vinna mikið með tengsl við önnur teymi, þar sem enska er allsráðandi og mikilvægt að það beri alþjóðlegt nafn. Sú hefð hefur skapast að gamla hugtakið CERT er töluvert notað í heitum CSIRT teyma, t.d. CERT-FI, NorCERT, CERT-BUND og CERT-DK. Í bili leggjum við til að þeirri hefð verði haldið áfram og teymið kallað IceCERT í erlendum samskiptum en t.d. „Miðstöð netvarna á Íslandi" hér heima.

Ef áherslan verður fyrst og fremst á samhæfingarmiðstöð, kemur heitið „Samhæfingarmiðstöð netvarna á ‚Íslandi" vel til greina og útlenska skammstöfunin yrði þá IceCERT/CC.

11 ÍSLENSKT ÞJÓÐAR-CSIRT – GREINING ÝMISSA ÞÁTTA[19]

HÉR VERÐUR GERÐ GREINING Á ÖÐRUM ÞÁTTUM, SVO SEM SAMSKIPTAMÁLUM, INNRA TÆKNIÖRYGGI, ÁHÆTTU Í REKSTRI, KRÖFUM TIL STARFSMANNA O.FL.

11.1 ÁHÆTTA Í UPPHAFI REKSTRAR

Eftirfarandi eru m.a. þær rekstrarhættur sem eru samfara stofnun þjóðar-CSIRT:

- Framlag uppfyllir ekki eftirspurn eftir þjónustu.
- Alvarleg veira, ormur, netárás eða annað öryggisatvik gæti komið upp um það leyti sem þjóðar-CSIRT tekur til starfa. Atvikið fengi mikla athygli hagsmunaaðila og fjölmiðla og vekti margar spurningar um hvernig teymið brást við.
- Margar leiðir eru til að vinna að net- og tölvuöryggi og ekki sjálfgefið að valin leið reynist sú besta.
- Þær upplýsingar sem safnast hafa geta tapast á einhvern hátt eða komist í rangar hendur, og er mikilvægt að verja þær á sem öruggastan hátt.

11.2 SAMSKIPTI OG ÍMYND

Nokkra mikilvæga þætti þarf að hafa í huga varðandi samskipti þjóðar-CSIRT við hagsmunaaðila sína og varðandi góða ímynd teymisins út á við. Nauðsynlegt er að gera samskiptaáætlun og innleiða hana á fyrstu stigum verkefnisins til að starfið beri árangur. Áætlunin gæti innihaldið eftirfarandi:

- Umfjöllun um væntingar við hagsmunaaðila.
- Áætlun um góðan samstarfsgrunn innan CSIRT áhrifasvæðisins, með því að hafa hagsmunaaðila með í ráðum frá upphafi.
- Útsendingu upplýsinga um störf, afurðir og gang verkefnisins.
- Áætlun um afgerandi jákvæða ímynd.

Lykilskilaboð í öllu sem kemur frá þjóðar-CSIRT er að það sé: Hlutlaust, sjálfstætt, fljótvirkt og traustur samstarfsaðili. Þjóðar-CSIRT þarf að halda úti eigin vefsíðu og gefa út bæklinga til kynningar á sér og starfsemi sinni.

Teymið heldur reglulega fundi fyrir þá sem sjá um tækni og upplýsingaöryggi hagsmunaaðila þess. Þar er rætt um stöðu mála og varnir hverju sinni. Þar að auki eru þessir aðilar á póstlista teymisins. Teymið hefur *þekkingarbanka* á vefsíðu sinni þar sem hagsmunaaðilar geta fundið ráðgjöf og greinar um upplýsingaöryggi og geta bætt við nýrri þekkingu.

[19] Margt unnið úr gögnum frá GovCERT í Hollandi

11.3 SAMSKIPTALEIÐIR

Mikilvægt er að samskiptaleiðir séu fastmótaðar, t.d.;

- Vörumerki, góð, afgerandi og áberandi mynd þess.
- Samræmt útlit á öllu sem kemur frá teyminu, svo sem á bréfsefni og glærukynningum.
- Vefsíða.
- Algengar spurningar og svör (FAQ).
- Almenn kynning.
- Byrja sýnilega, halda opnunarhátíð.
- Senda út mánaðarlegt eða ársfjórðungslegt fréttabréf.
- Vera með kynningar og takið þátt í ráðstefnum.
- Hafa skýra og ritaða stefnu um hvernig á að hafa samskipti við fjölmiðla og notfæra sér þá.
- Samskipti snúast um að samband við helstu hagsmunaaðila sé stöðugt og gott. Þar af leiðandi eru tvíhliða samskipti, þ.e. samskipti sem ganga í báðar áttir, við viðskiptamenn teymisins mikilvæg og efla sambönd og samvinnu.
- Gera lista yfir alla viðburði sem framundan eru og raða í forgang. Það kostar bæði tíma og erfiði að búa til góðar kynningar og fulltrúar teymisins þurfa að vera færir í að standa fyrir kynningum.
- Nýta aðrar samskiptaleiðir: Gerð efnis og yfirlestur kynninga og greina.
- Hafa hugfast að góð kynning vekur fólk til vitundar um starfsemi teymisins í heild.
- Það eru algeng mistök að gera ráð fyrir að allir í kring um mann hafi sömu tæknilegu þekkingu og skilning á hugtökum og maður sjálfur. Mjög mikilvægt er því að allt efni innihaldi eins lítið af flóknum tæknilegum orðum og hugtökum og mögulegt er.
- Aðrir möguleikar eru færir til þess að koma boðum áleiðis, svo sem útvarp og RSS streymi á vefsíðum.

11.4 SAMSKIPTI VIÐ FJÖLMIÐLA

Þjóðar-CSIRT teymið veitir fjölmiðlum viðtöl og upplýsingar um fréttnæm öryggisatvik líðandi stundar og um öryggismál í fjarskiptum almennt.

Einn valinn sérfræðingur þjóðar-CSIRT teymisins þarf að hluta til að starfa sem fjölmiðlafulltrúi. Ákjósanlegt er að hann sé vel inn í ógnum og hættum líðandi stundar, svo sem sérfræðingur sem meðhöndlar öryggisatvik. Þetta er mikilvægt starfssvið starfsmannsins og þjóðar-CSIRT teymisins í heild. Sérfræðingurinn þarf að vera andlit CSIRT út á við, koma vel fyrir og vera vel að sér í öryggismálum net- og tölvukerfa. Dæmi um efni samskipta við fjölmiðla eru m.a.:

- Almennar upplýsingar um netárásir í kjölfar öryggisatviks sem beint var að einstökum fjarskiptaleiðum, svo sem sæstrengjum til og frá landinu. Aftur á móti á teymið ekki að svara fyrir bilanir eða hvenær tiltekinni viðgerð líkur, slíkt er á ábyrgð fjarskiptafyrirtækjanna sjálfra.
- Tiltekin bilun getur komið af stað keðjuverkun öryggisatvika, t.d. ef bilun í netbeini veldur verulegri truflun sem veikir þær öryggisráðstafanir sem fyrir eru. Sem fyrr á fjarskiptafyrirtækið að tilkynna og veita frekari upplýsingar um sjálfa bilunina, svo sem áætlaðan viðgerðartíma og um áhrif bilunarinnar.
- Viðvaranir um öryggisatvik og öryggismál líðandi stundar.
- Fróðlegar upplýsingar um öryggisatvik og öryggismál almennt.

11.5 ÚTGÁFA EFNIS OG ÚTSELD ÞJÓNUSTA

Æskilegt er að þjóðar-CSIRT teymið gefi við og við út, þýði, eða mæli með, efni um netöryggismál fyrir hagsmunaaðila sína og fleiri, svo sem:

- Upplýsingar um þróun og tilhneigingar á sviði netglæpa, t.d. hvaða aðferðir njósnaglæpamenn notfæra sér hverju sinni. Þetta er góður stuðningur við aðvaranir og fréttatilkynningar.
- Hagnýtar upplýsingar svo sem greinar um njósnaforrit eða greinar um hvernig best er að afrita gögn.

Ennfremur getur þjóðar-CSIRT boðið útselda þjónustu við að sinna sértækum þörfum hagsmunaaðila sinna en þó í samræmi við starfsforsendur og skilyrði teymisins. Í slíkum tilfellum er æskilegt að gera samning við viðkomandi hagsmunaaðila þar sem sú þjónusta sem veita skal er nákvæmlega skilgreind og réttindi og skyldur beggja aðila tilgreind sem og kostnaður.

11.6 VITUNDARVAKNING OG AÐVARANIR TIL ALMENNINGS

Nokkur þjóðar-CSIRT teymi eru með á sinni könnu vitundarvakningu um tölvuöryggi fyrir sérfræðinga fjarskiptafyrirtækja og sérstaklega þá sem vinna við mikilvæga innviði sem varða þjóðaröryggi - sem sagt ekki við almenning. Þó eru einstaka dæmi þess að þjóðar-CSIRT séu með beina vitundarvakningu sem beinist að almenningi, svo sem gegnum sérstaka stoðdeild teymisins eða gegnum þriðja aðila. Seinna meir gætið þjóðar-CSIRT teymi veitt slíka þjónustu á sérstakri vefsíðu um öryggismál, sambærilegri við http://www.netöryggi.is.

Ennfremur er hugsanlegt að teymið aðvari almenning sérstaklega, beint eða óbeint, um alvarlega vá sem vofir yfir í íslenskum netkerfum en veita má þessa þjónustu gegnum vefsíðu teymisins og/eða gegnum þriðja aðila. Þetta síðasttalda er nefnt hér sem mögulegur valkostur er fram líða stundir, þótt það sé almennt ekki hluti af grunnstarfssemi þjóðar-CSIRT teyma.

11.7 AÐGENGI AÐ ÞJÓNUSTU, TÆKNI, STARFSFÓLKI OG AÐFERÐARFRÆÐI

Endursöluaðilar tæknibúnaðar á Íslandi eru yfirleitt vel í stakk búnir til að veita góða þjónustu og því oft hentugt að gera samning við þá um kaup og viðhald á búnaði.

Hugbúnaður CSIRT teyma er frekar sérhæfður og sérsmíðuð tæknitól tíðkast hjá þeim flestum. GovCERT í Hollandi hefur smíðað margskonar hugbúnað sem þeir láta öðrum í té endurgjaldslaust, ennfremur NorCert í Noregi. Dæmi um slíkt eru eftirlitskerfi, spilliforrita-skynjarar (malware sensors) sem er plantað í netum hér og þar, og tæknibúnaður til að stunda veikleikaprófanir (vulnerability tests).

Vélbúnaður er aftur á móti til á almennum markaði. Reikna má með að kaupa þurfi allan vélbúnað, bæði fyrir Windows og Linux stýrikerfi.

Á Íslandi er töluvert um hæfa tæknimenn og aðra starfsmenn sem gætu komið til starfa hjá þjóðar-CSIRT teyminu, bæði innan fjarskiptageirans og tölvutæknigeirans. CSIRT sérþekking ávinnst þó að mestu leyti í starfi og þurfa flestir tæknimenn að sækja námskeið erlendis í rekstri CSIRT teyma, t.d. Terena Transit námskeið.

11.8 AÐSTOÐ FRÁ ÚTLÖNDUM VIÐ GANGSETNINGU

Endursöluaðilar tæknibúnaðar á Íslandi og útlend CSIRT teymi eru yfirleitt mjög hjálpfús við að veita upplýsingar um aðferðarfræði sína, svo og um tæknibúnað í notkun.

ENISA (European Network Information Security Agency) er ennfremur með sérstaka deild sem stuðlar að aukinni CSIRT útbreiðslu innan EB og EFTA. Starfsemi deildarinnar er mest kynning, útgáfa og ráðstefnuhald um málefni CSIRT teyma. Þeir aðstoðuðu Litháa við uppsetningu á sínum þjóðar-CSIRT og getum við líklega leitað til þeirra um aðstoð og ráðgjöf við uppsetningu okkar þjóðar-CSIRT. Aðstoð þeirra getur þó verið fólgin í milligöngu um þau utanaðkomandi CSIRT teymi sem munu aðstoða og ráðleggja okkur.

11.9 INNRA TÆKNIÖRYGGI

Mikilvægt er að innra upplýsingakerfi þjóðar-CSIRT teymisins sé sem best úr garði gert og öryggið sett á oddinn. Huga þarf að eftirfarandi atriðum:

- Láta óháðan traustan aðila endurskoða öryggisstefnu, nethögun og tækjabúnað.
- Innleiða nauðsynlegar ráðstafanir sem lúta að leynd gagna, svo sem dulkóðun í afritunarmiðlum og geymslu þeirra utan starfssvæðis.
- Viðhafa öryggi í öllum nethögunarlögum innra netsins.
- Ekki treysta Interneti og öðrum ytri tengingum, t.d. forðast beintengingar frá Interneti við innra netkerfi.
- Merkja netkapla í mismunandi litum í samræmi við hlutverk, t.d. vinnslunet frá prufuneti.
- Viðhafa aðskilið prufunet og aldrei að samtengja til að fyrirbyggja mistök.
- Dulkóða gögn á diskum í fartölvum starfsmanna.
- Nota rafrænar undirskriftir og dulkóðun í samskiptum með tölvupósti.
- Greina það sem gæti farið úrskeiðis, nota bestu varnir og halda vöku sinni.
- Innleiða stefnu um viðreisn kerfa, t.d endurheimt afrita við diskhrun.
- Prófa reglulega afritunargögn.

11.10 VÖRSLUGÖGN OG TRÚNAÐUR MILLI AÐILA

Til þess að veita góða þjónustu þarf teymið mikið af traustum upplýsingum og að geta treyst þeim sem veita þær. Nauðsynlegt er að vita hvers kyns upplýsingar koma frá hverri upplýsingaveitu og meta það traust sem hægt er að bera til hverrar þeirra. Þjóðar-CSIRT mun m.a. meðhöndla eftirfarandi upplýsingar:

- Gögn um þekkt öryggisatvik í net- og upplýsingatækni – oft frá öðrum CSIRT.
- Trúnaðarupplýsingar milli teymisins og einstakra hagsmunaaðila.
- Gögn um samskipti, bæði innan lands og utan.
- Rannsóknargögn um nýja netvá.
- Mæligögn sem aflað er, m.a. við hugsanlega netvöktun. Margt af því er trúnaðarmál.
- Hugsanlegar net- og kerfismyndir sem fengnar eru frá fjarskiptafélögum.
- Hugsanlegar upplýsingar frá fjarskiptafélögunum um ástand og gæði net- og tæknikerfa þeirra.

11.11 MIKILVÆGI SKÝRSLUGERÐAR

Frá upphafi er mikilvægt að sýna hagsmuna- og fjármagnsaðilum fram á árangur verkefnisins, til dæmis:

- Hversu mörgum hagsmunaaðilum er þjónað.
- Hversu mikil ráðgjöf hefur verið veitt og hversu mikið hefur verið greitt fyrir hana
- Hversu margar tilkynningar/skýrslur um öryggisatvik hafa borist.
- Hvað annað sem hægt er að sýna fram á með einfaldri tölfræði, slíkt sparar tíma.
- Mikilvægt er að ábyrgðaraðili/ráðuneyti CSIRT sé látinn fylgjast vel með.

11.12 FYRIRTÆKJABRAGUR OG INNRA SKIPULAG

Æskilegt er að skipulag, vinnuferlar og fyrirtækjabragur séu þess eðlis að starfsemin og þjónustan sé sem áhrifaríkust. Eftirfarandi þættir stuðla að því:

- Flatt skipulag gefur teyminu sveigjanleika og pláss til að beina kröftum sínum í nýjar áttir og að nýjum þáttum í upplýsingatækni ef nauðsynlegt er.
- Leggja þarf áherslu á opin og hreinskiptin samskipti og vinnugleði starfsmanna. Það er mikilvægt fyrir teymi sem er í stöðugu sjálfsnámi að fólk hafi pláss til að gera mistök og læra af þeim. Teymið verður ekki fullvirkt nema virðing sé borin fyrir skoðunum hvers og eins.
- Æskilegt er að starfsmenn hafi reynslu af almennum vinnumarkaði. Slíkt fólk tekur mið af þeim sem þjónustan er veitt og er vant að vinna hratt úr nýjum hugmyndum. Ef unnið er með verktökum í upphafi gefur það góðan sveigjanleika en krefst markvissrar stjórnunar.
- Starfsmenn þurfa að vera sveigjanlegir og tilbúnir til að viðra eigin skoðanir.
- Ákveðin og skýr verkefnastjórnun er nauðsynleg á fyrstu stigum verkefnisins. Áætlanagerðin er mikilvægust og gott að hafa í huga að oft virkar best að taka lítil skref, og ekki má gleymast að fagna því þegar hverjum áfanga er náð. Einnig er nauðsynlegt að taka saman góðar áfangaskýrslur til að upplýsa stjórnvöld og vekja traust þeirra sem unnið er fyrir.

11.13 ALMENNAR KRÖFUR UM HÆFNI STARFSMANNA

Starfsmenn sem vinna við þjóðar-CSIRT þurfa að vera m.a. gæddir eftirfarandi eiginleikum:

- Sveigjanleiki, sköpunarkraftur og samstarfshæfni. Starfsmaður verður að geta brugðist við aðstæðum sjálfstætt og sem hluti af hóp.
- Hæfni til ákvarðanatöku og til að stýra tíma sínum í flóknum og krefjandi aðstæðum.
- Mikil greiningarhæfni. Starfsmenn þurfa að vinna með mikið magn af upplýsingum og verða bæði að hafa heildaryfirsýn og geta séð smæstu tæknilegu atriði þegar aðstæður krefjast þess.
- Mjög góð kunnátta í íslensku og ensku, talaðri og ritaðri.
- Hæfni til að meta upplýsingar og miðla tæknilegum upplýsingum til hagsmunaaðila eftir því sem við á.
- Góður skilningur á internettækni til að meta upplýsingar um áhættu og áhrif.
- Hæfni til að miðla flóknum tækniupplýsingum til þeirra sem hafa litla tæknilega þekkingu. Viðvaranir, kynningar og viðtöl við hagsmunaaðila þurfa að vera á máli sem allir geta skilið.
- Kunnátta í að höndla með viðkvæmar upplýsingar og vekja traust meðal hagsmunaaðila. Starfsmenn þurfa að vera með flekklausan feril og geta greint milli þess sem þarf að segja og ekki er nauðsynlegt að upplýsa um.
- Þekking á fjarskiptamarkaðinum

11.14 KRÖFUR TIL TÆKNIMANNA

Tæknimenn sem vinna við þjóðar--CSIRT þurfa að þekkja til eftirfarandi:

- Tækni almennt.
- Grunnatriði öryggis.
- Berskjöldun og veikleika í netum og kerfum.
- Þróun og sögu Internetsins.
- Áhættu við tölvuöryggi.
- Net-samskiptastaðla, svo sem IP, TCP, UDP, ICMP o.fl.
- Nafnakerfi (DNS).
- Netþjónustu og notkunarhugbúnað.
- Varnarráðstafanir.
- Stillingar búnaðar m.t.t. til öryggis.
- Hafa innsýn inn í tölvu-innbrotstækni.
- Dulkóðunartækni.
- Hugbúnaðargerð.

Þeir þurfa jafnframt að hafa hæfileika til að vinna við greiningarvinnu, t.d. greiningu á berskjöldun/veikleika neta og kerfa.

11.15 MENNTUN STARFSMANNA

Tæknimenn sem vinna í þjóðar-CSIRT þurfa stöðugt að vera vel að sér í nýjustu tækni hvers tíma og hver stefnan er í þeim efnum. Þeir þurfa að sækja ráðstefnur, símenntunarnámskeið og fundi í útlöndum. Ennfremur er mikilvægt að heimsækja önnur útlend CSIRT teymi og taka á móti heimsóknum.

Menntun nýrra starfsmanna er lykilatriði í upphafi starfsins. Reynsla CERT-FI er sú að það tekur um hálft ár fyrir nýjan starfsmann að verða virkur í starfi. TERENA (Transit training) veitir frekar ódýr 2ja daga námskeið fyrir nýja starfsmenn CSIRT teyma og senda mörg CSIRT teymi nýja starfsmenn sína þangað.

11.16 OPNUNAR- OG VIÐBRAGÐSTÍMI

Sá tími dagsins sem starfsemi hinna ýmsu CSIRT teyma er opin er mismunandi, t.d. alla virka daga, átta tíma á dag (5x8) og allt að 24/7/365 sólarhringsvaktir. Þegar um sólarhringsvaktir er að ræða eru tæknimenn yfirleitt á bakvöktum og geta brugðist snöggt við ábendingum úr eftirlitskerfum eða símhringingum. Minni CSIRT ráða ekki við að halda úti sólarhringsvöktun og gerum við því ráð fyrir 5x8 (virka daga, átta tímar á dag) til að byrja með. Smátt og smátt má svo bæta við bakvöktum, ef svo ber undir.

Ekki er óeðlilegt að viðbragðstími, þ.e. sá tími sem það tekur starfsmenn að hefja rannsókn eða byrja vinnu á tilteknu nýju öryggisatviki, sé innan 2ja klukkustunda.

11.17 FJÖLDI STARFSMANNA

Fjöldi starfsmanna fer eftir ýmsum þáttum, svo sem þeirri þjónustu sem boðin er, loforð um viðbragðstíma og sá tími sólarhringsins sem starfsemin er virk, t.d. hvort sólarhringsvaktar sé krafist árið um kring eða bakvakta. Ennfremur skiptir máli reynsla og þekking starfsmanna, áætlaður fjöldi öryggisatvika og alvarleiki þeirra. Síðast en ekki síst skiptir fjármagn miklu varðandi mannaráðningar. Reynslan frá útlöndum sýnir þó að lágmarki þarf 4-5 starfsmenn íþjóðar-CSIRT. Margir byrja með 4 starfsmenn í fullu starfi en flestir þeirra hafa þurft að auka fjöldann innan árs. Í Noregi, Svíþjóð, Finnlandi og Hollandi eru t.d. 15-18 starfsmenn í þeirra forystu-CSIRT teymum.

Þjóðar-CSIRT þeirra örfáu landa sem hafa 3 starfsmenn og færri hafa þurft að vinna náið með öðrum þjóðum. Dæmi um þetta er Eistland sem vinnur náið með Finnlandi. Þar voru starfsmenn tveir og lentu í því að ráða illa við vandamál sem komu upp í netkerfum landsins. Í kjölfarið var fjölgað í fjóra.

Ekki vita höfundar skýrslunnar um þjóðar-CSIRT sem vill láta taka sig alvarlega og er með 3 eða færri starfsmenn.

Af vel mönnuðum CSIRT má taka sem dæmi CERT-FI í Finnlandi sem er með eftirtalið starfslið; 8 tæknimenn, einn yfirmann, 6 í notendaþjónustu og 2 lögfræðinga – samtals eru þetta 18 manns sem þeir hafa til reiðu en starfsmenn notendaþjónustunnar sinna líka .fi landslénamálum fyrir eftirlitsstofnunina FICORA.

Starfsemi CSIRT er þannig að ekki er stöðugt verið að kljást við öryggisatvik, ekki frekar en stjórnstöð almannavarna er stöðugt að sinna útköllum björgunarsveita. En starfsemin þarf að ráða við öryggisatvik þegar þau koma upp. Á milli stríða skipuleggja tæknimenn sig, t.d. með undirbúningi, vitundarvakningu og fræðslu um þessi mál. Lögfræðingar sinna margs konar lögfræðilegum þáttum. Þess vegna mælum við með að lágmarki fimm fastráðnum starfsmönnum til að byrja með, þar af a.m.k. þremur tæknimönnum en þeim þarf yfirleitt að fjölga fljótlega. *Ef starfsemin nær ekki til mikilvægra innviða fjarskipta- og upplýsinganeta er varðar þjóðaröryggi, má reikna með a.m.k. einu stöðugildi færra.*

Sjá nánar hugsanlegt fyrirfram skilgreint ábyrgðarsvið hvers og eins starfsmanns í viðauka A.

11.18 LAGALEGIR ÞÆTTIR

Auk þess sem skilgreint er sem dagleg/venjuleg verkefni þurfa lögfræðingar og sérfræðingar að huga að eftirfarandi við stofnun þjóðar-CSIRT:

- Skilgreina lagalegan grundvöll og tilgreina hver verkefni, geta og ábyrgð teymisins eru.
- Gera lista yfir þau lög og reglur sem geta haft áhrif á starfsemina.
- Sjá til þess að tekið sé tillit til allra viðeigandi laga og reglna í starfseminni.
- Útbúa nákvæman lista yfir staðlaða þjónustu og þau skilyrði sem miðað er við.
- Gera yfirlit yfir sértæka þjónustu eins og mögulegt er.

Ekki er ólíklegt að setja þurfi sérstakar reglur eða reglugerð, til að skerpa rammann utan um fyrirhugaða starfsemi.

11.19 TÍMAMÖRK

Gera má ráð fyrir að það taki a.m.k. 8-9 mánuði frá því að starfsmenn hefja störf þar til þjóðar-CSIRT tekur til starfa. Sá tími fer í margs konar undirbúning, þ.m.t. ákvarðanir um búnað og gangsetningu, þjálfun starfsmanna, kynningarstarf o.fl. Lauslega má gera eftirfarandi tímaáætlun þar sem gert er ráð fyrir að fyrir liggi útlistuð áætlun um starfssemina:

- 0-3 mánuðir - skipulagning
- 3-9 mánuðir – innleiðing ferla og kerfa

- 9 mánuðir – upphaf fyrstu starfsemi sem síðan eykst stig af stigi

Stöðugt þurfa starfsmenn að vera í samstarfi við utanaðkomandi aðila. *Sjá nánar fimm hagnýt áfangaþrep í viðauka C fyrir þá sem vinna að stofnun þjóðar-CSIRT.*

12 KOSTNAÐUR

HÉR VERÐUR GERÐ LAUSLEG KOSTNAÐARGREINING Á MISMUNANDI ÚTFÆRSLUM ÞJÓÐAR-CSIRT TEYMA.

12.1 AUKAKOSTNAÐUR OG SKIPTING

Ekki er óeðlilegt að viðkomandi stofnanir eða samstarf innan tengdra fyrirtækja greiði ákveðinn hluta af kostnaði við einn starfsmann sem sinnir málefnum mikilvægra innviða. Starfsmaðurinn myndi sinna þessum málaflokki eingöngu og fá við það aðstoð annarra starfsmanna teymisins, svo sem tæknimanna og skrifstofufólks. Reikna má með að þessi hluti starfseminnar sé 40% af heildarstarfsemi þjóðar-CSIRT. Sums staðar er hlutfallið hærra.

12.2 KOSTNAÐARGREINING ÞJÓÐAR-CSIRT – IP FJARSKIPTANET OG AÐRIR INNVIÐIR

Væntingar neytenda snúast um aukið öryggi, jafnt í netviðskiptum sem í daglegri netnotkun. Þjóðar-CSIRT þarf að styðja við hagsmunaaðila sína sem kemur íslenskum neytendum til góða, en frumskilyrði er að nægar tekjur og nægt fjármagn sé til staðar fyrir starfsemina. Fyrst þegar búið er að ákveða endanlegt fyrirkomulag og starfsemi þjóðar-CSIRT er hægt að gera nákvæma kostnaðargreiningu. Eftirfarandi gefur þó fyrstu mynd af kostnaði þjóðar-CSIRT með Internet og aðra mikilvæga innviði á sinni könnu.

Stofnkostnaður

Gera má lauslega ráð fyrir eftirfarandi útlistun á fjármagnsþörf við stofnun fyrsta árið:

- Kaup á vélbúnaði – kr. 3 mj.*
- Kaup á margs konar hugbúnaði – kr. 2,5. mj.
- Heimasíða, m.a. með viðvörunarþjónustu – kr. 1,5 mj.
- Kynningarefni, ársleiga, skrifstofubúnaður o.fl. – kr. 5 mj.
- Námskeið erlendis fyrir starfsmenn – kr. 2 mj.
- Launakostnaður fimm starfsmanna – er á bilinu 35 mj.**

Samtals kostar því fyrsta árið frá 49 mj. kr.

Rekstrarkostnaður

Þegar teymið hefur verið stofnað má lauslega gera ráð fyrir eftirfarandi rekstrarkostnaði á ári:

- Viðhald og endurnýjun tækniumhverfis – kr. 2 mj.*
- Kynningarstarfsemi og fræðsla 3 mj.
- Leiga, skrifstofukostnaður – 2 mj.
- Námskeið, fundarhöld og námskeið starfsmanna – 2 mj.
- Launakostanaður fimm starfsmanna – er á bilinu 35 mj.**

Samtals er árlegur rekstrarkostnaður um 42 mj. kr.

*Tölvur starfsmanna, sérhæfðar kerfisvélar, margskonar hugbúnaður og uppsetning.

**Laun og launatengd gjöld starfsmanns, ásamt ferðakostnaði 2-3 á ári til útlanda, áætlum við 7 mj. á ári, þ.e.a.s. 35 mj. fyrir 5 starfsmenn. Í ofangreindri áætlun er gert ráð fyrir að starfsemin nái til mikilvægra innviða er varða þjóðaröryggi.

12.3 KOSTNAÐARGREINING ÞJÓÐAR-CSIRT – IP FJARSKIPTANET EINVÖRÐUNGU

Eftirfarandi gefur fyrstu mynd af kostnaði þjóðar-CSIRT með Internet og önnur IP fjarskiptanet einvörðungu á sinni könnu.

Stofnkostnaður

Gera má lauslega ráð fyrir eftirfarandi útlistun á fjármagnsþörf við stofnun fyrsta árið:

- Kaup á vélbúnaði – kr. 3 mj.*
- Kaup á margs konar hugbúnaði – kr. 1,5. mj.
- Heimasíða, m.a. með viðvörunarþjónustu – kr. 1,5 mj.
- Kynningarefni, ársleiga, skrifstofubúnaður o.fl. – kr. 5 mj.
- Námskeið erlendis fyrir starfsmenn – kr. 2 mj.
- Launakostnaður fjögurra starfsmanna – er á bilinu 28 mj.**

Samtals kostar því fyrsta árið frá 41 mj. kr.

Rekstrarkostnaður

Þegar teymið hefur verið stofnað má lauslega gera ráð fyrir eftirfarandi rekstrarkostnaði á ári:

- Viðhald og endurnýjun tækniumhverfis – kr. 2 mj.*
- Kynningarstarfsemi og fræðsla 3 mj.
- Leiga, skrifstofukostnaður – 2 mj.
- Námskeið, fundarhöld og námskeið starfsmanna – 2 mj.
- Launakostanaður fjögurra starfsmanna – er á bilinu 28 mj.**

Samtals er árlegur rekstrarkostnaður um 37 mj. kr.

*Tölvur starfsmanna, sérhæfðar kerfisvélar, margskonar hugbúnaður og uppsetning.

**Laun og launatengd gjöld starfsmanns, ásamt ferðakostnaði 2-3 á ári til útlanda, áætlum við 7 mj. á ári, þ.e.a.s. 28 mj. fyrir 4 starfsmenn. Í ofangreindri áætlun er ekki gert ráð fyrir að starfsemin nái til mikilvægra innviða er varða þjóðaröryggi.

12.4 KOSTNAÐARGREINING ÞJÓÐAR-CSIRT - EINGÖNGU SAMHÆFINGARMIÐSTÖÐ

Til að lækka kostnað kemur til greina að reka eingöngu hluta starfsemi fullútbúins þjóðar-CSIRT, þ.e. binda starfsemina við samhæfingarmiðstöð og samskiptamiðstöð gagnvart Internet tengdum öryggisatvikum og annarra IP fjarskiptaneta. Við þessa breytingu má gera ráð fyrir að nokkrir þættir detti út, svo sem margs konar rannsóknarvinna. Starfsemin hefur þá væntanlega eftirfarandi kostnað í för með sér.

Stofnkostnaður

Gera má lauslega ráð fyrir eftirfarandi útlistun á fjármagnsþörf við stofnun fyrsta árið:

- Kaup á vélbúnaði – kr. 2 mj.*
- Kaup á margs konar hugbúnaði – kr. 1,0. mj.
- Heimasíða, m.a. með viðvörunarþjónustu – kr. 1,5 mj.
- Kynningarefni, ársleiga, skrifstofubúnaður o.fl. – kr. 3 mj.
- Námskeið erlendis fyrir starfsmenn – kr. 1,5 mj.
- Launakostanaður þriggja starfsmanna – er á bilinu 21 mj.**

Samtals kostar því fyrsta árið frá 30 mj. kr.

*Tölvur starfsmanna, sérhæfðar kerfisvélar og uppsetning.

Rekstrarkostnaður

Þegar teymið hefur verið stofnað má lauslega gera ráð fyrir eftirfarandi rekstrarkostnaði á ári:

- Viðhald og endurnýjun tækniumhverfis – kr. 1,5 mj.*
- Kynningarstarfsemi og fræðsla 1 mj.
- Leiga, skrifstofukostnaður – 1,5 mj.
- Námskeið, fundarhöld og námskeið starfsmanna – 1 mj.
- Launakostanaður þriggja starfsmanna – er á bilinu 21 mj.**

Samtals er árlegur rekstrarkostnaður um 26 mj. kr.

*Tölvur starfsmanna, sérhæfðar kerfisvélar, margskonar hugbúnaður og uppsetning.

**Laun og launatengd gjöld starfsmanns, ásamt ferðakostnaði 2-3 á ári til útlanda, áætlum við 7 mj. á ári, þ.e.a.s. 21 mj. fyrir 3 starfsmenn.

Í ofangreindri áætlun er ekki gert ráð fyrir að starfsemin nái til mikilvægra innviða er varða þjóðaröryggi. Þó má gera ráð fyrir að kostnaður haldist nokkurn veginn óbreyttur að öðru leyti en því að við bætist a.m.k. eitt stöðugildi.

13 FJÁRMÖGNUN

Fjármögnunarleiðir

Mismunandi er eftir löndum hvernig þjóðar-CSIRT eru fjármögnuð. Dæmi eru um að fjármagn komi frá eftirtöldum aðilum í mismunandi útfærslum:

- Hið opinbera, t.d. viðkomandi ráðuneyti og/eða hlutfall af rekstri eftirlitsstofnunar.
- Hagsmunaaðilar t.d. fjarskiptafyrirtæki sem hlutfall af veltu.
- Bankar og fjármálastofnanir eða fjármálageirinn í heild sinni.
- Aðrir atvinnugeirar, svo sem samgöngur, orkugeirinn, verslun, menntastofnanir o.s.frv.
- Almannavarnir.
- Þeir aðilar sem sjá um rekstur hvers konar mikilvægra innviða þjóðfélagsins er varða þjóðaröryggi, svo sem ábyrgðaraðilar neyðarbirgða, samganga o.fl.
- Tekjur teymisins við sérverkefni, fræðslu o.fl.

13.1 VAL Á FJÁRMÖGNUNARLEIÐ

Eins og fyrr greinir eru ýmsar leiðir farnar við fjármögnun þjóðar-CSIRT. Fjármögnun er m.a. háð þeirri þjónustu sem veitt er og hverjir eru hagsmunaaðilar teymisins. Þó ber að hafa í huga að teymið sé sem óháðast við val á verkefnum og forgangi þeirra. Setja má spurningamerki við hvort bein fjárframlög frá hagsmunaaðilum geri það að einhverju leyti háðari þeim við val á verkefnum. Á móti kemur að greiðslur skapa oft aukið traust milli aðila. Eftirtaldar fjármögnunarleiðir koma m.a. til greina við hið íslenska þjóðar-CSIRT:

- Lágmarkskrafa er að þjóðar-CSIRT stuðli að vernd gegn öryggisatvikum á Internetinu. Ef það verður látið duga gæti fjármögnunarleiðin verið eftirfarandi:
    - Frá hinu opinbera, s.s. samgönguráðuneyti og/eða Póst- og fjarskiptastofnun

- Í framhaldi af ofansögðu og með tilliti til þess hversu smár íslenski fjarskiptamarkaðurinn er, kemur til greina að hagsmunaaðilarnir leggi sitt af mörkum og hlutfallsleg skipting orðið eftirfarandi:
    - 20% frá hinu opinbera, s.s. samgönguráðuneyti og/eða Póst- og fjarskiptastofnun
    - 80 % frá hagsmunaaðilum, t.d. fjarskiptafyrirtækjum

- Ef þjóðar-CSIRT verður jafnframt látið stuðla að vernd gegn öryggisatvikum í mikilvægum fjarskipta- og upplýsingainnviðum fjarskiptageirans, svo og annarra atvinnugeira, svo sem orku- og fjármálageirans, gæti hlutfallsleg skipting orðið eftirfarandi:
    - 60% frá hinu opinbera, s.s. samgönguráðuneyti og/eða Póst- og fjarskiptastofnun

- 40 % frá einstökum aðilum/stofnunum sem bera ábyrgð á mikilvægum innviðum þjóðfélagsins er varða þjóðaröryggi, þ.e. fjármálaráðuneyti, samgönguráðuneyti, heilbrigðisráðuneyti, iðnaðarráðuneyti og hugsanlega frá fleirum.

- Ef við bætast menntastofnanir, svo sem rannsóknarstofnanir og háskólar, má reikna með 10% kostnaðarhlutdeild þeirra:
  - 50% frá hinu opinbera, s.s. samgönguráðuneyti og/eða Póst- og fjarskiptastofnun
  - 40 % frá einstökum aðilum/stofnunum sem bera ábyrgð á mikilvægum innviðum þjóðfélagsins er varða þjóðaröryggi, þ.e. fjármálaráðuneyti, samgönguráðuneyti, heilbrigðisráðuneyti, iðnaðarráðuneyti og hugsanlega frá fleirum.
  - 10% frá menntastofnunum, svo sem frá HÍ, HR og hugsanlega menntamálaráðuneyti.

Til að byrja með teljum við næst síðasta kostinn vera ákjósanlegastan.

14 ÞRÍR VALKOSTIR HÉR Á LANDI

ÞEGAR UPP ER STAÐIÐ ERU EFTIRFARANDI ÞRÍR VALKOSTIR UM STARFSEMI CSIRT HÉR Á LANDI ÞEIR HELSTU. STUÐST ER VIÐ FYRRI KOSTNAÐARGREININGU.

14.1 VEL ÚTBÚIÐ ÞJÓÐAR-CSIRT – INNVIÐIR IP FJARSKIPTANETA OG AÐRIR INNVIÐIR

Vel útbúið þjóðar-CSIRT, sem jafnframt innviðum Internetsins hefur á sinni könnu málefni annarra mikilvægra innviða fjarskipta- og upplýsinganeta, svo sem fastlínusíma. Starfsemi, kostnaður og annað yrði eftirfarandi:

Starfsemi:

- Samhæfingarmiðstöð netvarna á landsvísu í fjarskipta- og upplýsinganetum.
- Samskiptamiðstöð í samstarfsneti meðal hagsmunaaðila, við útlönd, og við aðra tengda aðila.
- Viðvörunarþjónusta.
- Styðja við skráningu öryggisatvika innanlands.
- Leiða atvika-, veikleika- og búnaðargreiningu, ásamt því að dreifa upplýsingumum atvik og berskjölduð tölvu- og fjarskiptakerfi.
- Taka þátt í alþjóðlegu samstarfi um öryggi Internetsins.
- Aðstoða hagsmunaaðila sína við að auka eigin færni í að stjórna meðhöndlun öryggisatvika.
- Þýða efni um öryggismál yfir á íslensku, t.d. rannsóknir á spilliforritum o.fl.
- Veita aðgengilegar upplýsingar og ráð um öryggismál.
- Styðja við, eða taka þátt í áætlun um námsþjálfun, vitundarvakningu og þjálfunarefni sem hentar hinum ýmsu hópum þjóðfélagsins.
- Viðhalda skráningu á verksviði og færni annarra CSIRT teyma innanlands, ásamt tengiliðum.
- Viðhalda öllu ofangreindu fyrir innviði aðra en IP fjarskiptanet, svo sem fastlínu og farsímakerfa.

Fimm starfsmenn, t.d.:

- Forstöðumaður
- Þrír tæknimenn
- Eða tveir tæknimenn og einn lögfræðingur
- Skrifstofuhald

Kostnaður:

- Stofnkostnaður: 49 mj.
- Árlegur rekstrarkostnaður: 42 mj.

Tekið skal fram að ofangreind áætlun um starfsmenn á við upphaf starfseminnar. Reynsla annarra ríkja sýnir að starfsmönnum er fljótlega fjölgað. Þrír er æskilegur lágmarksfjöldi tæknimanna .

14.2 VEL ÚTBÚIÐ ÞJÓÐAR-CSIRT – INNVIÐIR IP FJARSKIPTANETA EINVÖRÐUNGU

Vel útbúið þjóðar-CSIRT, sem hefur undir sínum verndarvæng innviði IP fjarskiptaneta, svo sem Internetsins á Íslandi;

Starfsemi:

- Samhæfingarmiðstöð netvarna á landsvísu gagnvart Interneti og öðrum IP fjarskiptanetum.
- Samskiptamiðstöð í tengslaneti meðal hagsmunaaðila, við útlönd, og við aðra tengda aðila.
- Viðvörunarþjónusta.
- Styðja við skráningu öryggisatvika innanlands.
- Leiða atvika-, veikleika- og búnaðargreiningu, ásamt því að dreifa upplýsingum um atvik og berskjölduð tölvu- og fjarskiptakerfi.
- Taka þátt í alþjóðlegu samstarfi um öryggi Internetsins.
- Aðstoða hagsmunaaðila sína við að auka eigin færni í að stjórna meðhöndlun öryggisatvika.
- Þýða efni um öryggismál yfir á íslensku, t.d. rannsóknir á spilliforritum o.fl.
- Veita aðgengilegar upplýsingar og ráð um öryggismál.
- Styðja við, eða taka þátt í áætlun um námsþjálfun, vitundarvakningu og þjálfunarefni sem hentar hinum ýmsu hópum þjóðfélagsins.
- Viðhalda skráningu á verksviði og færni annarra CSIRT innanlands, ásamt tengiliðum.

Fjórir starfsmenn, t.d.:

- Forstöðumaður
- Tveir tæknimenn
- Skrifstofa ofl.

Kostnaður:

- Stofnkostnaður: 41 mj.
- Árlegur rekstrarkostnaður: 37 mj.

14.3 SAMHÆFINGARMIÐSTÖÐ ÞJÓÐAR-CSIRT – INNVIÐIR IP FJARSKIPTANETA

Samhæfingar- og samskiptamiðstöð (SOS) sem samhæfir aðgerðir og samskipti, þegar upp koma alvarleg öryggisatvik í íslenskum IP netkerfum. Starfsemi, kostnaður og annað yrði eftirfarandi:

Starfsemi:

- Samhæfingarmiðstöð netvarna á landsvísu gagnvart Interneti og öðrum IP fjarskiptanetum.
- Samskiptamiðstöð í tengslaneti meðal hagsmunaaðila, við útlönd, og við aðra tengda aðila.

Þrír starfsmenn, t.d.:

- Forstöðumaður og tæknimaður.
- Tæknimaður.
- Símsvörun og bókhald.

Kostnaður:

- Stofnkostnaður: 30 mj.
- Árlegur rekstrarkostnaður: 26 mj.

Starfsemi teymisins er hægt að útvíkka seinna meir í átt að víðtækara starfssviði skv. ofangreindu.

Tekið skal fram að allar ofangreindar tölur um kostnað, gefa eingöngu lauslega mynd af kostnaði.

15 ORÐASKÝRINGAR

Orðaskýringar

Almenn fjarskipti: Fjarskipti sem standa almenningi til boða.

AS númer: AS tölum/númerum er úthlutað af RIPE (www.ripe.net) til netrekenda í þeim tilgangi að lýsa á auðveldan hátt hvernig viðkomandi fjarskiptafélag ákveður að skiptast á IP umferð við nágranna-net sín gegnum netbeina. Notkun þeirra felur í sér lýsingu á stefnu (Routing Policy) sem hvert og eitt fjarskiptafyrirtæki setur sér, í þeim tilgangi að marka brautir (paths) sem umferðinni er beint eftir. Sérhverju AS númeri tilheyra IP-net, þ.e. röð IP vistfanga (einnig úthlutað af RIPE) sem allar falla undir sömu beinireglur (þ.e. beinireglur AS-tölunnar).

Mikilvægir innviðir er varða þjóðaröryggi (CI-Critical Infrastructure): Innviðir þjóðfélagsins er varða þjóðaröryggi, svo sem orkugeirinn, olíudreifing, brigðamál o.fl.

Mikilvægir innviðir fjarskipta er varða þjóðaröryggi (CII-Critical Information Infrastructure): Innviðir í fjarskipta- og upplýsingatækni í ýmsum geirum þjóðfélagsins þar sem öryggisatvik, ótrygg virkni eða tortryggileg atvik geta varðað þjóðaröryggi, t.d. haft áhrif á aðra innviði þjóðfélagsins, stofnað öryggi almennings í hættu, ógnað efnahagslegu og þjóðfélagslegu jafnvægi eða valdið óstöðugleika í stjórn og vörnum landsins.

Netárás: Árás í gegnum fjarskiptanet, sem miðar að því að skerða þjónustu eða trufla virkni neta og kerfa. Árásin getur verið margslungin ef beitt er mismunandi netvopnum. Hún getur komið frá einu vistfangi (DoSA-Denial of Service Attack) eða átt sér upptök hjá mörgum IP vistföngum samtímis (DDoSA-istributed Denial of Service Attack) sem veikir netvarnir.

Netvarnir: Eldveggir og önnur tiltæk ráð sem eru notuð við að verjast netárásum.

Netvopn: Hugbúnaður, skipanir og önnur tól og tæki sem notuð eru við að gera netárásir á Internetinu. Netvopnin geta verið allt frá stöðluðum tölvuskipunum sem hleypa af stað runu af gagnapökkum, s.s. PING skipun, til sérhannaðs hugbúnaðar sem sendir runu gagnapakka sem innihalda skemmdarmátt og falsaðar upprunaupplýsingar, í þeim tilgangi að laska viðkomandi búnað sem árásinni er beint gegn.

Íslensk netkerfi: Netkerfi sem hýsa öll AS númer á Íslandi, eða sem er stjórnað af íslenskum aðilum, lénanöfn sem hafa endinguna .is, símanet sem tilheyra +354 landanúmeri og öll önnur net í eigu eða rekstri íslenskra aðila.

Íslensk netþjónusta: Netþjónusta sem veitt er á Íslandi eða af íslenskum aðilum.

Laumunet: – Botnet eða Zombie valda hvað mestri tímaeyðslu og ama hjá flestum tölvunotendum. Með þessari aðferð hafa tölvuþrjótar hafa náð að planta spilliforriti, svokölluðu "Bot" laumuforriti (dregið af “Robot”) í allstóran hóp heimilistölva grunlausra eigenda og bæta þeim inn í sitt laumunet (Botnet). Þannig búa þeir til net tölva sem þeir geta virkjað allar í einu. Laumuforrit sérhverrar tölvu bíður frekari fyrirmæla, þangað til þrjóturinn tekur til við að fjarstýra þeim öllum í einu til ýmissa óheillaverka. Þessu má líkja við hóp uppvakninga sem er sendur af stað, og þaðan er orðið Zombie komið. Oft eru þessi net leigð út þrjótum á t.d. 100 dollara í nokkrar klukkustundir. Frá laumunetum er stærstur hluti alls ruslpósts sendur út á Internetið (Bulk SPAM), þau geyma og nota netvopn til DDoSA netárása og þau eru gróðrarstía forrita sem skráir niður allan lyklaborðs-innslátt og sendir til þrjótanna (keyloggers).

Netlögsaga: Það mengi AS-númera sem tilheyra íslenskum aðilum, er skilgreint hér sem netlögsaga Íslands.

Ógn: Hugsanleg orsök óæskilegs atviks sem getur valdið skaða á kerfi eða fyrirtæki.

Rótarmein: (RootKit) svipar til laumuforrita (bot) en eru ólík þeim að því leyti að veiruvarnir finna þau yfirleitt ekki. Ástæðan er sú að þeim er komið fyrir djúpt í stýrikerfinu og geta m.a. lokað fyrir að veiruvarnir og aðrar varnir tölvunnar vinni rétt, þótt þau virðist vera í lagi og fullvirk. Þau geta ennfremur fylgst með netnotkun og yfirtekið stjórn á tölvunni. Til að uppgötva og losna við rótarmein þarf yfirleitt að nota sérhönnuð leitarforrit, þar sem hefðbundnar varnir duga ekki til, eða setja stýrikerfið á ný inn í tölvuna.

Röskunarþol: (Resilience) Viðmið um getu fjarskiptaneta til að veita lágmarks viðeigandi þjónustu, þegar öryggisatvik og önnur áföll dynja yfir í fjarskiptanetunum eða annars staðar í þjóðfélaginu – Röskunarþol eykur seiglu í fjarskiptanetunum gegn þessum þáttum. Það er samspil regluverks og óbundinna aðferða og tæknilegra ráðstafana, sem ná til margra hluta innviða þjóðfélagsins. Í heildarmyndinni er æskilegt að taka tillit til alls þessa, frekar en einblína t.d. á tæknilegar ráðstafanir.

Þjóðar-CSIRT: "Computer Security and Incident Response Team" er forystuhópur sem stuðlar að vernd gegn öryggisatvikum, ótryggri virkni og tortryggilegum atvikum í fjarskipta- og upplýsinganetum í sínu landi. M.a. sinnir teymið forvörnum, er í viðbragðsstöðu og aðstoðar hagsmunaaðila sína með viðbrögð gegn öryggisatvikum.

Þjónustusynjun: Synjun þjónustu eða skerðing, af völdum truflana, bilana eða netárása.

Öryggisatburður: Það að upp kemur staða kerfis, þjónustu eða nets sem gefur til kynna hugsanlegt brot gegn öryggisstefnu eða bilun í öryggisráðstöfun, eða þá áður óþekkt staða sem getur skipt máli fyrir öryggi.

Öryggisatvik: Atvik sem er gefið til kynna með einum eða fleiri óæskilegum eða óvæntum öryggisatburðum sem talsverðar líkur eru á að stofni rekstrarþáttum í hættu og ógni upplýsingaöryggi.

16 HEIMILDIR OG NOKKUR FRUMGÖGN

- Fjarskiptaáætlun fyrir árin 2005-2010. Samgönguráðuneytið árið 2005 – ISBN 9979-9402-4-7.
- Skýrsla starfshóps samgönguráðherra um öryggi fjarskipta o.fl. Samgönguráðuneytið nóvember 2006.
- ENISA – A step-by-step approach on how to set up a CSIRT (Deliverable WP2006/5.1 CERT-D1/D2),
- ENISA – CERT cooperation and its further facilitation by relevant stakeholders (Deliverable WP22006/5.1 CERT-D3).
- GOVCERT - 'CERT-in-a-Box' and 'Alerting service-in-a-Box' - Des. 2005
- Carnegie Mellon Software Engineering Institute – Steps for creating National CSIRTs – Ágúst 2004.
- Carnegie Mellon Software Engineering Institute – State of the Practice of Computer Security Incident Response Teams (CSIRTs) – Okt. 2003
- RFC 2350 - Expectations for Computer Security Incident Response
- Ýmsar upplýsingar og gögn sem aflað var í fundum með CERT-FI, ENISA og Terena TF-CSIRT.

17 VIÐAUKI A - ÝMSAR ÚTFÆRSLUR CSIRT TEYMA[20]

17.1 FYRIRKOMULAG STARFSEMINNAR OG TENGSL VIÐ GRASRÓTINA

Fyrirkomulag starfsemi CSIRT getur verið breytilegt, svo sem:

- Miðlægt CSIRT
- Landfræðilega dreift CSIRT

Breytileg nálgun getur verið við grasrótina:

- Mannskapur CSIRT veitir ráð og samhæfir aðgerðir hagsmunaaðila sinna sem stilla sjálfir búnað og viðhafa aðrar öryggisráðstafanir gagnvart öryggisatvikum, þ.e. þeir nálgast grasrótina í ákveðinni fjarlægð ofan frá (Top-Down).
- Mannskapur CSIRT fer á staðinn til að "slökkva elda" innan áhrifasvæðis síns, þ.e. vinnur beint í grasrótinni (Bottom-Up).

17.2 FLOKKUN Í SAMRÆMI VIÐ TILGANG, VIRKNI OG ÞJÓNUSTU

Ennfremur er algengt að flokka CSIRT í samræmi við tilgang, virkni og þjónustu, skv. eftirtöldu:

- Innri CSIRT aðila svo sem fyrirtækja, banka, háskóla eða stofnunar, sem samræmir eða meðhöndlar öryggisatvik í þágu þess aðila sem rekur teymið.
- Samhæfingarmiðstöð fyrir CSIRT sem samhæfir og auðveldar meðhöndlun öryggisatvika meðal annarra CSIRT teyma, innan tiltekins lands, innan rannsóknarseturs eða á hliðstæðu sviði. Oftast eru samhæfingarmiðstöðvar með vítt starfssvið og CSIRT áhrifasvæðið víðfeðmt.
- CSIRT teymi framleiðenda hugbúnaðar- eða vélbúnaðar sem koma upplýsingum á framfæri um galla í vöru þeirra. Þessir aðilar rannsaka gallana, koma endurbótum á framfæri og dreifa til viðskiptavina eða almennings. Slík CSIRT vinna með öðrum öryggis- og rannsóknarhópum, svo og öryggissérfræðingum, í þeim tilgangi að koma auga á gallana og endurbæta framleiðsluna.
- Netþjónustur starfrækja stundum CSIRT sem viðskiptavinir þeirra hafa aðgang að gegn gjaldi. Segja má að þetta sé "stjórnuð öryggisþjónustuveita".
- CSIRT þar sem greiningardeildin er höfuðáhersla starfseminnar, þ.e. teymið einblínir á samantekt gagna frá mismunandi stöðum, í þeim tilgangi að ákvarða mynstur og í hvaða farveg öryggisatvik leita í hvert sinn. Slíkar upplýsingar má nýta er framtíð öryggismála er skoðuð. Ennfremur við að veita viðvörun í upphafi þegar fyrstu ummerki um nýja ógn samræmist fyrirfram ákveðnum hættumerkjum.

[20] Unnið úr gögnum frá CERT/CC og GovCERT

17.3 CSIRT FLOKKUÐ EFTIR HAGSMUNAAÐILUM

17.3.1 CSIRT FYRIR LÍTIL OG MEÐALSTÓR FYRIRTÆKI/STOFNANIR

- Þessi teymi bera ábyrgð á litlum og meðalstórum fyrirtækjum og stofnunum sem af einhverjum ástæðum geta ekki sett upp eigin teymi og eru upplýsingakerfi þeirra innan CSIRT áhrifasvæðisins.
- Geta starfað eingöngu fyrir sitt fyrirtæki eða vinna fyrir hóp fyrirtækja.
- Hagsmunaaðilar á áhrifasvæðinu geta verið litlu eða meðalstóru fyrirtækin, starfsmenn þeirra, eða aðilar sem tengjast afmörkuðu málefni, t.d. allar bæjarstjórnir á Íslandi.
- Slík teymi vinna yfirleitt beint í grasrótinni, þ.e. stjórna sjálfir netum og öðrum búnað.

17.3.2 CSIRT FYRIR HÁSKÓLA- OG FRÆÐIGEIRANN

- Þessi teymi bera ábyrgð á mennta- og rannsóknarstofnunum og –stofum, og eru upplýsingakerfi þeirra innan áhrifasvæða þeirra, t.d. innra netkerfi.
- A.m.k. tvö slík eru bæði í Noregi og Finnlandi.
- RHnet á Íslandi er skráð sem slíkt teymi en er ekki með virka starfsemi.
- Hagsmunaaðilar eru starfsmenn og nemendur í háskólum og framhaldsskólum.
- Breytilegt er hvort þau vinna beint eða óbeint í grasrótinni.

17.3.3 CSIRT Á SVIÐI HERNAÐAR- OG VARNARMÁLA

- Þessi teymi bera ábyrgð á tölvu- og netkerfum sem notuð eru til þjóðvarna. Hagsmunaaðilarnir samanstanda af stofnunum á sviði hernaðar og önnur tengd starfsemi, t.d. varnarmálaráðuneyti og þær stofnanir ríkisins sem tengjast þeim.

17.3.4 CSIRT FYRIR STOFNANIR SEM SINNA MIKILVÆGUM INNVIÐUM

- Mikilvægir innviðir skipa háan sess hjá ríkisstjórnum. Þess vegna hefur víða verið komið á sérstökum og sérhæfðum CSIRT sem leggja áherslu á vernd mikilvægra upplýsingakerfa innviðanna sem eru innan áhrifasvæða þessara teyma.
- Þau styrkja og auka varnir tölvu- og netkerfa á áhrifasvæði sínu, og þar með virkni samfélagsins.
- Teymið hefur náin tengsl við þær stofnanir eða ráðuneyti, sem fara með sérhvern málaflokk um mikilvæga innviði.
- Með hliðsjón af stærð og fjölda slíkra stofnana gæti verið skynsamlegt að skilgreina sér CSIRT fyrir mismunandi málaflokka innviðanna, svo sem fyrir:
    - Fjarskipta- og upplýsingageirann (CIIP)
    - Fjármálageirann
    - Samgöngur
    - Orku- og vatnsgeirann
    - Heilbrigðis- og öryggisþjónustu
- Hagsmunaaðilarnir eru stjórnvöld og þeir aðilar sem reka hvers konar mikilvæga þjónustu fyrir samfélagið sem byggist á upplýsingatækni, og almennir borgarar.

17.3.5 STJÓRNSÝSLU-CSIRT

- Þetta teymi starfar fyrir stjórnsýslustofnanir með hliðsjón af skipulagi og skilgreiningum stofnana í hverju landi og nær til ráðuneyta, stofnana og skrifstofa í ríkisgeiranum og jafnvel á sviði sveitarstjórnar.
- Markmið teymisins er að styðja viðhald á innviðum tölvu- og nettækninnar hjá stjórnsýslunni og styrkja framboð á rafrænni þjónustu innan stjórnsýslugeirans.
- Þótt það sé ekki hans kjarnastarfssemi, virkar slíkt teymi stundum sem mið- og tengipunktur, svipað og þjóðar-CSIRT gerir.
- Dæmi um stjórnsýslu-CSIRT er GOVCERT í Hollandi.
- Hagsmunaaðilinn er stjórnsýslan í heild sinni.
- Stundum teygja þessi teymi sig í átt til þess að sinna almenningi líka, t.d. í Belgíu, Ungverjalandi, Hollandi, Bretlandi og Þýskalandi.

17.3.6 ÞJÓÐAR-CSIRT

- Þjóðar-CSIRT hefur öryggi fjarskipta og upplýsingakerfa þjóðarinnar í heild sinni að leiðarljósi. Þegar öryggisatvik verða er þetta CSIRT mið- og tengipunktur fyrir öll önnur slík teymi, sem og stofnanir og einstaklinga í landinu og þá sem senda inn viðbragðsbeiðni að utan.
- Þjóðar-CSIRT samræmir aðgerðir landsins gegn öryggisatvikum.
- Á CSIRT áhrifasvæði sínu hefur teymið undir sínum verndarvæng önnur CSIRT í landinu og aðra þá stærri aðila sem gera þjónustusamning við teymið þar að lútandi.
- Eitt helsta hlutverk þess er ofangreint milligönguhlutverk fyrir þjóðina í heild sinni.
- Þjóðar-CSIRT nálgast grasrótina ofan frá, þ.e. eru ráðgefandi.
- Þessi teymi útvíkka stundum starfsemi sína. Dæmi um slík teymi eru CERT-FI í Finnlandi með aukinni verndarþjónustu í tengslum við upplýsingakerfi sem almenningur nýtir sér og NorCERT í Noregi í átt til verndar upplýsingakerfa sem tengjast hernaði.

17.3.7 CSIRT Á ALMENNUM MARKAÐI

- Slíkt teymi sinnir hverjum þeim sem greiðir fyrir þjónustuna. Þar sem teymið þarf að fjármagna starfsemi sína með þeim hætti þarf það einnig að lúta almennum reglum um starfsemi á almennum markaði. Þar af leiðandi er slíkt teymi “arðsækið” og gerir samninga við hvern viðskiptavin. Það leiðir aftur af sér að samvinna slíkra teyma við önnur CSIRT er takmörkuð (þ.e. teymið má ekki deila upplýsingum með þriðja aðila).
- Net- og þjónustuveita getur rekið slíkt teymi fyrir viðskiptavini sína.
- Hagsmunaaðilar eru þeir sem kaupa þjónustuna, t.d. almennir endanotendur net- og þjónustuveitna og notendur þeirra sem flokkast sem fagaðilar í upplýsingatækni.

17.3.8 CSIRT FYRIR SÖLUAÐILA

- Slík teymi sinnir þeim sem selja tiltekna vöru á markaði. Markmið þess er venjulega að hanna og útvega lausnir til að auka varnir sölukerfa eða a.m.k. draga úr hugsanlegum neikvæðum þáttum slíkra kerfa.
- Hagsmunaaðilar eru eigendur starfseminnar og CSIRT áhrifasvæðið upplýsingakerfi þeirra

17.3.9 INNRI CSIRT

- Slíkt teymi sinnir þjónustu við móðurfélag sitt, t.d. banka eða fjarskiptafyrirtæki.
- Viðfangsefni teymisins er vernd upplýsingakerfa móðurfélagsins.
- Teymið vinnur yfirleitt í grasrótinni, þ.e. gerir sjálft lagfæringar og stillingar í búnaði upplýsingakerfanna.
- Teymið rekur yfirleitt ekki vefsíðu sem er opin almenningi.
- Innan CSIRT áhrifasvæðisins geta verið tæknikerfi móðurfélagsins, þ.m.t. starfsmenn tölvudeilda móðurfélagsins og upplýsingakerfi þess.

18 VIÐAUKI B - HLUTVERK OG ÁBYRGÐ STARFSMANNA[21]

18.1 FRAMKVÆMDASTJÓRI EÐA HÓPSTJÓRI

- Stýrir stefnumörkun.
- Stýrir og skipuleggur vinnu meðlima teymisins.
- Er verkstjóri teymisins.
- Er fulltrúi CSIRT gagnvart framkvæmdastjórn og öðrum.
- Sér um starfsmannaviðtöl og ráðningar á meðlimum/starfsmönnum teymisins.

18.2 AÐSTOÐARFRAMKVÆMDASTJÓRAR, VERKSTJÓRAR EÐA HÓPSTJÓRAR

- Koma að stefnumörkun á ákveðnum sviðum.
- Styðja stjórn CSIRT eftir þörfum.
- Leiðbeina og fræða starfsmenn teymisins eftir þörfum.
- Deila verkefnum á starfsmenn.
- Taka þátt í viðtölum við nýja starfsmenn teymisins.

18.3 STARFSMENN ÞJÓNUSTUBORÐSSÍMA, HJÁLPARLÍNU EÐA Í PRÓFUNUM

- Sjá um aðalsíma CSIRT teymisins.
- Veita aðstoð í upphafi eftir sem þeir hafa kunnáttu til.
- Sjá um skráningu upplýsinga í upphafi og flokkun og forgangsröðun innkomandi upplýsinga.

18.4 STARFSMENN SEM MEÐHÖNDLA ÖRYGGISATVIK

- Sjá um greiningu atvika, að rekja þau, skráningu og viðbrögð.
- Samræma leiðbeiningar sem teymið sendir frá sér um viðbrögð og aðgerðir við öryggisatvikum. (þ.e. útbúa leiðbeiningarefni, svo sem um hvernig skrá eigi atvik, gátlista og góðar verklagsreglur).
- Dreifa upplýsingum.
- Eru í samskiptum við CSIRT, utanaðkomandi sérfræðinga og aðra (svo sem vefsetur, fjölmiðla, lögreglu eða lögfræðinga) eftir þörfum og eins og tiltekið er af stjórnendum CSIRT.
- Sjá um tæknilega vöktun ef kveðið er á um slíkt.
- Þróa viðeigandi efni til þjálfunar (fyrir starfsfólk CSIRT og/eða þiggjendur þjónustunnar).
- Leiðbeina og fræða nýja starfsmenn eins og ákvæði eru um.
- Fylgjast með skynjarakerfi fyrir netárásir ef slíkt er hluti af starfi CSIRT.
- Sjá um prófanir á innflæði ef slíkt er hluti af starfi CSIRT.
- Taka þátt í viðtölum við nýja starfsmenn ef um það er beðið.

18.5 STARFSMENN SEM FYLGJAST MEÐ VEIKLEIKUM Í KERFUM

- Greina, prófa, rekja og skrá veikleikaskýrslur og rannsaka hugsanlega laskaðan tækjabúnað eftir netmisferli.
- Rannsaka eða þróa úrbætur og viðgerðir.

[21] Unnið úr gögnum frá GovCERT

- Hafa samskipti við þjónustuþiggjendur, CSIRT, framleiðendur hugbúnaðar, utanaðkomandi sérfræðinga og aðra (fjölmiðla, lögreglu eða lögfræðinga) eftir þörfum.
- Dreifa upplýsingum um veikleika og tilheyrandi úrbætur, viðgerðir og verkferla.
- Sjá um tæknilega vöktun ef kveðið er á um slíkt.
- Leiðbeina og fræða nýja starfsmenn eins og ákvæði eru um.
- Taka þátt í viðtölum við nýja starfsmenn.

18.6 TÆKNILEGIR RITARAR/RITSTJÓRAR

- Aðstoða og hvetja CSIRT við útgáfu á efni, svo sem leiðbeiningum, góðum verklagsreglum eða ábendingum um tæknileg atriði.

18.7 VEFHÖNNUÐIR OG VEFSTJÓRAR

- Sjá um vefsetur CSIRT.
- Sjá um gerð nýs efnis og útlits fyrir vefinn í samráði við starfsfólk CSIRT.
- Stjórna vefumsjónarbúnaði.
- Viðhalda innviðum vefsins, vinna náið með öðrum kerfis-/netstjórum.

18.8 KENNARAR/ÞJÁLFARAR

- Þróa og útbúa námsefni til að þjálfa nýja starfsmenn CSIRT í meðhöndlun öryggisatvika.
- Þróa og útbúa námsefni fyrir þiggjendur þjónustunnar.
- Leggja til þjálfun til að efla öryggisvitund.

18.9 NET- OG KERFISSTJÓRAR

- Hafa umsjón með búnaði CSIRT og aðtengdum tækjum.
- Viðhalda tæknilegum innviðum í starfi CSIRT, svo sem öruggum netþjónum, gagnaskrám, öruggum póstþjónum og hvaða öðrum búnaði sem teymið þarfnast í starfi sínu.

18.10 STARFSMENN Í STOÐÞJÓNUSTU

- Aðstoða aðra starfsmenn á sviði tækni eða stjórnunar eins og þörf er á.
- Samræma skipulag ferða starfsmanna á ráðstefnur, námskeið eða fundi eins og þörf er á.

18.11 SÉRFRÆÐINGAR VÉL- OG STÝRIKERFA

- Aðstoða við greiningu atvika og viðbrögð við þeim með því að leggja til sérfræðiþekkingu á sviði mismunandi tæknibúnaðar og kerfa (t.d. UNIX, Windows, stórtölvum, notkunarhugbúnaðar, gagnagrunna).
- Geta einnig séð um meðhöndlun öryggisatvika, veikleika eða verkefni sem snúa að tæknilegum innviðum ef þörf er á.

19 VIÐAUKI C – HAGNÝTAR UPPLÝSINGAR VEGNA UPPBYGGINGAR ÞJÓÐAR-CSIRT[22]

19.1 MYNDUN ÞJÓÐAR-CSIRT Í FIMM ÞREPUM.

Reynslan af myndun þjóðar-CSIRT annarsstaðar hefur sýnt fram á að gott er að skipta ferlinu niður í fimm meginþrep. Eftirfarandi upplýsingar eru komnar frá CERT/CC og lýsa ferlinu í myndun teymisins frá því að hugmyndin að því verður til þar til teymið er orðið fullvirkt. Þótt munur sé á því hvernig vinna fer fram frá degi til dags eru ákveðnir þættir í myndunarferlinu sem eru sameiginlegir öllum slíkum teymum.

Þessi fimm þrep draga upp skýra mynd af því hvað þarf til að mynda þjóðar-CSIRT; frá því að áætlanagerð hefst til þess að komið hefur verið á ákveðnum ferlum í meðferð öryggisatvika. Í þessum þrepum felst m.a. að skilgreina þá hagsmuna- og samstarfsaðila sem koma að myndun teymisins, gera verkefnisáætlun og setja fram sýn á það hvernig teymið verður skipulagt og byggt upp, hvernig starfsmannahaldi verður háttað, hvernig starf teymisins verður fjármagnað, þjálfun starfsfólks og innleiðing þess gangverks sem nota á til að meta og bæta starfsemina.

Á öllum stigum getur komið fyrir að stíga þarf skref til baka og afla upplýsinga sem ekki var fyrirséð að þyrfti þegar vinnan hófst. Þetta á bæði við um ný CSIRT og þau sem þegar hafa hafið störf. Dæmi um þetta er þegar ráða þarf nýtt starfsfólk í teymi sem þegar hefur hafið störf. Þá þarf að veita því fólki grunnþjálfun svo það skilji hlutverk og ábyrgð teymisins. Annað dæmi er ef breytingar verða á því umhverfi sem teymið vinnur í. Slíkt getur leitt til þess að teymið þarf að stíga skref til baka og endurskoða áætlun sína, markmið og vinnulag.

Hér á eftir verður farið yfir þessi fimm þrep; kynning, áætlanagerð, innleiðing, starfsemi og samstarf, sem nýtast ættu þeim sem hafa fengið það hlutverk að mynda þjóðar-CSIRT.

19.2 ÞREP 1 – TILURÐ OG TILGANGUR ÞJÓÐAR-CSIRT KYNNT

Á þessu stigi er um vakningarátak að ræða þar sem þeir aðilar sem þurfa að koma að samstarfi við teymið eða taka þátt/standa að kynningu á eðli þess og starfi eru fræddir um hvað felst í að mynda slíkt teymi sem þjóna skal þjóðinni allri; hvaða ákvarðanir þarf að taka, hlutverk teymisins (t.d. sem miðpunktur meðferðar, viðbragða og upplýsinga um öryggisatvik) og önnur mikilvæg atriði sem þarf að huga að, svo sem hvernig starfsemin skuli skipulögð, hvernig teymið skuli mannað, hvernig koma skal á öruggum samskiptaleiðum, nauðsyn á samræmingu viðbragða og aðgerða lykilaðila o.s.frv.

[22] Unnið úr gögnum frá CERT/CC

Til viðbótar því að nýta þá menntun og þjálfun sem almennt er fyrir hendi í samfélaginu til kynningar á tilurð og tilgangi CSIRT er nauðsynlegt að halda fundi og koma af stað umræðum um hag samfélagsins af því að hafa slíkt teymi og hvaða styrk það þarf að hafa. Á fundum og í umræðum ætti t.d. að ræða:

- Hvaða viðskiptaþættir og hagsmunir það eru sem mynda þörfina fyrir þjóðar-CSIRT. Hér er átt við þau lög og reglur sem við eiga, hvaða mikilvægu innviði samfélagsins þarf að vernda, hvers kyns atvik eða árásir geta átt sér stað sem ógna öryggi eða hagsmunum samfélagsins, o.s.frv.
- Hvað felst í því að mynda CSIRT sem hefur styrk til að bregðast við á þjóðarvísu. Þ.e. hvaða regluverk þarf til, skilgreining á þeim aðilum sem þarf að vernda, hvað þarf til að teymið geti starfað, svo sem búnað og mannafla og hvernig byggja þarf upp innviði starfsins, hvernig á að fjármagna starfið, hvernig koma skal á samstarfi milli mismunandi aðila og að setja þurfi skýra öryggisstefnu og vinnureglur.
- Hvaða fólk þarf að koma að undirbúningi þess að mynda þjóðar-CSIRT. Hverjir þurfa koma að því að þróa og kynna teymið og hverjir ættu koma að áætlanagerð og innleiðingu starfseminnar. Þarna gæti verið um að ræða valda fulltrúa stjórnsýslunnar, bæði frá ráðuneytum og stofnunum, fulltrúa stofnana sem tengjast mikilvægum innviðum samfélagsins, fulltrúa aðila sem sinna öryggismálum í samfélaginu, fulltrúa aðila úr atvinnulífinu, fulltrúa CSIRT sem sinna afmörkuðum sviðum (t.d. sveitarfélögum, stofnunum eða fyrirtækjum), fulltrúa fyrirtækja á sviði tækni- og öryggisbúnaðar, sérfræðinga, fulltrúa löggjafarvaldsins og lögfræðinga, fulltrúa fjölmiðlafólks, fulltrúa fólks úr viðskiptalífinu og fólks úr fjarskipta- og upplýsingatæknigeiranum, svo dæmi séu nefnd.
- Skilgreiningar á hverjar eru helstu auðlindir og burðarstoðir samfélagsins
- Skilgreiningar á þeim samskiptaleiðum sem horfa þarf til, ekki aðeins til að auðvelda samvinnu og samræmingu í uppbyggingarferli teymisins, heldur einnig síðar þegar það er orðið virkt, til að samskipti og samvinna gangi sem best og öruggast fyrir sig.
- Hvaða markmiðum og árangri stefnt skal að í starfi teymisins og hverjar væntingarnar eru.
- Skilgreiningar á því lagaumhverfi og regluverki sem setja ramma um starf teymisins, svo sem hömlur á starfsemi, umboð, verndun upplýsinga og eftirfylgni.
- Hvernig hægt sé fjármagna myndun og starf teymisins
- Skilgreiningar á tækni, búnaði og netuppbyggingu sem þarf til að þjóðar-CSIRT geti starfað.
- Umræður um grunnviðbrögð við netvá, hvernig þau snerta mismunandi aðila samfélagsins og tengsl þeirra (stjórnsýslan, viðskiptalífið, menntakerfið o.s.frv.).
- Skilgreina þá grunnþjónustu sem þjóðar-CSIRT á að veita.
- Vandleg skoðun á því hvernig aðrar þjóðir standa að myndun þjóðar-CSIRT og mat á hvaða aðferðir virka best og hvað af þeim er hægt að tileinka sér í myndunarferli teymisins.

19.3 ÞREP 2 – ÁÆTLUN UM MYNDUN ÞJÓÐAR-CSIRT

Þegar þeirri þekkingu og upplýsingum sem fengist hafa í 1. þrepi hefur verið safnað saman er næsta skref að gera áætlun um myndun og starfsemi CSIRT. Það sem nú þarf að ræða er t.d. hvernig setja skal fram með skýrum hætti þörfina fyrir slíkt teymi og hlutverk þess, skilgreina helstu hagsmunaaðila, skilgreina þá þjónustu og stuðning sem það á að veita, meta fjármagnsþörfina, gera tímasetta verkefnisáætlun um myndun teymisins og finna fólkið sem fær það hlutverk að stýra myndun þess þar til það er orðið að veruleika og farið að starfa.

Aðgerðir á þessu stigi eru m.a.:

- Útlistun á þörfinni fyrir þjóðar-CSIRT og hvers skal krafist af því. M.a. þarf að safna upplýsingum um:
    - Lög og reglur sem munu hafa áhrif á starfsemi þjóðar-CSIRT.
    - Þá þætti samfélagsins sem skilgreindir eru sem mikilvægir og þarf að vernda.
    - Atvik og tilhneigingar í netglæpum sem eru að koma upp og hafa verið tilkynnt eða ætti að tilkynna.
    - Hvaða öryggisúrræði og sérþekking á sviði netöryggis eru þegar fyrir hendi.
    - Hvar í samfélaginu vantar úrræði og ferla til að bregðast við öryggisatvikum.
    - Þróa skýra sýn á hvernig CSIRT á að starfa. Í því felst að:
        - Skilgreina verkefni þess.
        - Skilgreina þá aðila sem teymið á að þjóna.
        - Skilgreina hvaða samskiptaleiðir milli CSIRT og þeirra sem það þjónar þurfa að vera fyrir hendi (hvað leiðir eru til og hvað þarf að búa til eða aðlaga).
        - Skilgreina þá þjónustu sem teymið á að veita (þ.e. viðvaranir og tilkynningar, þýðingarþjónusta, greining atvika, samræming viðbragða við öryggisatvikum, greining á styrk- og veikleikum, mat á öðrum CSIRT sem þegar starfa í samfélaginu, þjálfun í öryggisvakningu o.s.frv.).
        - Gera skipulagsrit fyrir teymið og skilgreina hvaða umboð það hefur, hvar það mun hafa starfsstöð og hvaða öryggiskröfur þarf að gera til starfsumhverfis þess.
        - Skilgreina þörf fyrir mannafla, búnað og aðra innviði.
        - Meta fjármagnsþörf og skilgreina hvaðan fjármagnið á að koma. Fjármögnunarleiðir geta t.d. verið þjónustugjöld, þjónustusamningar, fjármagn frá ríkinu, greiðslur fyrir fræðilega vinnu eða rannsóknir, samstarfssamningar, áskriftargjöld eða blönduð fjármögnun. Til viðbótar við kostnað við myndun og uppsetningu teymisins og starfsumhverfis þess þarf að undirbúa langtíma fjármögnun.
        - Skilgreina staðsetningu teymisins í ríkiskerfinu, hverjir stýra því og hvaðan stuðningur þarf að koma til að teymið nái árangri.
        - Skilgreina hvaða hæfni og kunnáttu starfsfólk teymisins þarf að hafa.
        - Skilgreina hlutverk og ábyrgð þjóðar-CSIRT; hvaða verkefnum á sinna, hver á að sinna þeim, hvenær og við hvaða aðstæður, hvernig á að skrá viðfangsefni, eftirfylgni, eftirlit o.s.frv.
        - Skilgreina hvernig brugðist er við öryggisatvikum, þ.e. gera ferlislýsingar um undirbúning, varnir, eftirlit og viðbrögð. Einnig þarf að skoða hvernig þessi ferli tengjast samskonar ferlum hjá einstökum aðilum innan hagsmunateymisins.

- Staðla viðmiðanir og hugtakanotkun til að auðvelda flokkun og skilgreiningar á öryggisatvikum og meðferð og viðbrögðum við þeim.
- Gera leiðarvísi um hvernig bregðast skuli við öryggisatvikum og hvernig þau skuli tilkynnt. Einnig þarf að gera skýra lýsingu á hvernig samskiptum við hagsmunahópinn, önnur CSIRT í samfélaginu og alþjóðleg teymi skuli háttað.
- Skilgreina tengsl, samskiptaferli og samvinnu við þau öryggiskerfi sem fyrir eru í samfélaginu og á alþjóðavísu.
- Skilgreina þær hömlur sem kunna að hafa áhrif á myndun og starfsemi teymisins.
- Skilgreina aðferðir til að byggja upp traust í samskiptum og gera samninga um samvinnu við lykilaðila og þá sem bera ábyrgð á mikilvægum innviðum í samfélaginu.
- Skilgreina samskiptaleiðir og -reglur og hvernig upplýsingum skuli miðlað (tölvupóstur, vefsíður, útgáfa skýrslna eða aðrar leiðir).
- Gera tímaáætlanir fyrir verkefnið og ákveða hvenær ákveðnum þáttum skuli vera lokið.
- Gera verkefnisáætlun fyrir teymið sem byggist á undirbúningsvinnunni, sýn á hlutverk teymisins og skilgreiningu á umhverfi þess; fá viðbrögð og gagnrýni utanfrá og nýta til að endurskoða áætlanir eins og nauðsynlegt er, gera tímaáætlanir um endurskoðun og breytingar á verkefnisáætluninni og öðrum gögnum sem tengjast myndun teymisins.

Undirbúningsteymið gæti sett fram skjal með “hugmyndafræði” teymisins til að styðja við afmörkun verkefnisins og skilgreina ábyrgð. Slíkt skjal yrði leiðarvísir við framsetningu á “sýn” teymisins og drægi fram helstu þættina sem talað er um hér að ofan. Í skjalinu væri einnig að finna upplýsingar um leiðarljós og reglur, samhæfingarhlutverk og –ábyrgð, hvernig samskiptum við aðra skuli háttað, s.s. miðlun upplýsinga og leiðbeininga.

19.4 ÞREP 3 - INNLEIÐING CSIRT

Á þessu stigi notar undirbúningshópurinn upplýsingar sem fengist hafa í þrepunum á undan til að setja upp og innleiða starfsemi þjóðar-CSIRT.

Þetta gerist í nokkrum þrepum, m.a.:

- Tryggja fjármagn frá aðilum sem búið er að skilgreina og ræða við í undirbúningsferlinu. Hér er komið að því að fjármagn verði aðgengilegt.

- Almenn kynning á því að verið sé að koma á þjóðar-CSIRT og hvar hægt sé að nálgast nánari upplýsingar (t.d. um hverjir komi að teyminu, hvernig tilkynningum og upplýsingaflæði verði háttað o.s.frv.)
- Formgera samhæfingar- og samskiptaferli gagnvart öllum aðilum sem teymið þarf að vinna með, veita upplýsingar eða hafa samskipti við. Þetta felur m.a. í sér að tilnefna tengiliði, setja reglur um hvaða upplýsingar verði bundnar trúnaði, hvaða upplýsingar verði nauðsynlegar, setja dulkóðunarstaðla, gera leiðarvísi um upplýsingaflæði milli aðila, o.s.frv.
- Innleiða örugg upplýsingakerfi og samskiptanet fyrir teymið (svo sem örugga netþjóna, notkunarhugbúnað, viðmót, fjarskiptatækni og aðra mikilvæga innviði).
- Gerð framkvæmdastefnu og ferlislýsinga fyrir starfsfólk teymisins.
- Framsetning á stefnu teymisins og gerð reglna um aðgang og notkun þess búnaðar sem teymið hefur yfir að ráða sem og notkunarreglur.
- Innleiða samskiptareglur CSIRT við hagsmunaaðila.
- Finna og ráða starfsfólk, veita því viðeigandi þjálfun og fræðslu og skilgreina aðferðir til að fræða og þjálfa þá sem teymið á að þjóna.

19.5 ÞREP 4 – STARFSEMI CSIRT HEFST

Þegar starfsemi hefst er komin grunngeta til meðferðar á öryggisatvikum, teymið farið að taka við tilkynningum um atvik og samræma viðbrögð við þeim.

Þau verkefni sem hafa verið skilgreind á stigum áætlanagerðar og innleiðingar hafa nú bæði form og innihald. Þjóðar-CSIRT hefur skýra sýn á hlutverk sitt og ákveðinn vinnuramma þar sem skilgreind eru markmið og áherslur, skipulag, umboð, fjármögnun, auðlindir og mikilvægar stoðir.

Stefna og ferlar hafa verið skilgreind og innleidd, m.a. aðferðir til að halda traustu sambandi við allra hagsmunaaðila, ferlar til að tryggja öruggar samskiptaleiðir, áætlanir um samræmingu og greiningu atvika og viðbragða, aðferðir við að milda áhrif öryggisatvika og aðferðir við miðlun upplýsinga til viðkomandi hagsmunaaðila í hverju tilfelli.

Helstu hagsmunaaðilar og aðrir sem njóta þjónustu CSIRT, þ.á m. sérfræðingar, hafa samþykkt þjóðar-CSIRT teymið, þekkja það og treysta því.

Skýrar reglur um miðlun upplýsinga, samræmingu aðgerða og stigmögnun í viðbrögðum við ógnunum í netöryggi og hindrun netárása hafa verið kynntar og innleiddar.

Þjóðar-CSIRT hvetur til og styður stofnun annarra CSIRT innan samfélagsins með því að leggja til og deila skjölum, áætlunum, formum fyrir ferlislýsingar, leiðbeiningum, þjálfun og upplýsingum sem ætlaðar eru til vitundarvakningar, auk hvers kyns annars efnis sem að notum getur komið (t.d. á opinni vefsíðu).

Verkefni teymisins á þessu stigi eru m.a.:

- Virk starfsemi.
- Þróun og innleiðing aðferða til að meta árangur þjóðar-CSIRT. Þetta gerir kleift að meta getu teymisins til að mæta þeim kröfum sem gerðar eru til þess og tryggja að það nái markmiðum sínum og sinni þörfum samfélagsins.
- Bæta starfsemina í framhaldi af niðurstöðum mats.
- Víkka út verkefnið, auka þjónustuna og fjölga starfsfólki eftir því sem þarf og hægt er að standa undir til að bæta þjónustu við hagsmunaaðila (t.d. þýðingarþjónusta og aukning á greiningarþjónustu og rannsóknum).
- Viðvarandi vöktun á öllum breytingum sem verða á hópi hagsmunaaðila, lagaumhverfi, stefnu stjórnvalda eða regluverki sem gætu haft áhrif á verkefnið og markmið þess í heild. Skilgreina þarf aðferðir til að gera breytingar á starfseminni ef þess þarf til að bæta skilvirkni og árangur.
- Þjálfun og fræðsla nýrra og eldri starfsmanna í starfsreglum, reglum um meðferð öryggisatvika, tilhneigingum á sviði netárása, aðferðum og tækjum til að milda afleiðingar árása. Einnig tryggja stöðugt flæði traustra upplýsinga og fræðslu, t.d. með símenntun starfsmanna.
- Stöðug þróun og áhersla á að bæta stefnu og starfsemi þjóðar-CSIRT.

19.6 ÞREP 5 – SAMVINNA

Virkur CSIRT viðheldur og þróar starfsemi sína sífellt og er um leið að sinna stöðugri uppbyggingu traustra sambanda og samskipta við helstu hagsmunaaðila, samstarfsaðila og önnur CSIRT. Þroskað CSIRT hefur starfað í einhvern tíma og hefur marktæka reynslu í meðferð öryggisatvika. Það nýtur trausts meðal annarra CSIRT á alþjóðavísu og hefur komið sér upp marktækum og traustum starfsaðferðum til að finna og bregðast við ógnunum sem að steðja á Netinu og milda eða koma í veg fyrir áhrif þeirra.

Aðgerðir á þessu stigi eru m.a.:

- Samstarf um miðlun og dreifingu gagna og upplýsinga og þátttaka í stöðlun meðferðar þeirra.
- Þátttaka í alþjóðlegu starfi um vöktun og viðvaranir við netvá. Þetta styrkir starf heima fyrir.
- Aukning á gæðum starfseminnar með því að veita þjálfun, standa fyrir vinnusmiðjum og ráðstefnum þar sem rætt er um tilhneigingar í netglæpum og viðbragðsáætlanir.
- Samvinna við aðra í samfélaginu um þróun kynningarefnis og leiðbeininga um bestu aðferðir til vernda öryggi í mikilvægum innviðum. Einnigþróun viðbragðsáætlana.
- Stöðug endurskoðun og endurbætur á meðferð öryggisatvika til að bæta árangur. Allar breytingar í þjónustu CSIRT þarf að kynna rækilega.
- Stuðla að þróun CSIRT teyma innan mikilvægra stofnana og sviða samfélagsins og þjóna sem fyrirmynd þeirra um starfsaðferðir. Þjóðar-CSIRT gæti einnig tekið að sér árangursmat og afkastaprófanir fyrir þessi teymi, jafnvel vottað starfsemi þeirra og veitt viðurkenningar.

20 VIÐAUKI D – DÆMI UM STJÓRNSÝSLU-CSIRT – GOVCERT Í HOLLANDI[23]

GOVCERT.NL (www.govcert.nl) teymið í Hollandi er stjórnsýslu-CSIRT en sinnir þar að auki viðvörunarþjónustu fyrir almenning. Það má því segja að heildarstarfsemin líkist að mörgu leyti þjóðar-CSIRT. Teymið hefur gefið út góð gögn um starfsemina og er þessi kafli byggður á þeim.

Teymið hóf störf í júní árið 2002. Eftir 6 mánaða vinnu þar sem gerð var verkáætlun og settur saman listi yfir helstu þiggjendur þjónustunnar hóf teymið störf. Megin markmið þess er að tryggja gæði í þjónustu og upplýsingagjöf á sem stystum tíma.

Teymið veitir sólarhringsþjónustu sem skiptist í tvær vaktir. Full starfsemi er á dagvakt frá kl. 9:00 – 23:00. Bakvakt með GSM síma er á nóttunni frá 23:00 – 9:00. Á dagvakt er farið yfir alla upplýsingabrunna, vefsíður, póstlista og aðrar upplýsingar. Ef eitthvað mikilvægt kemur upp gefur tæknilegur sérfræðingur út leiðbeiningar. Starfsmaður á "þjónustuborði" fer yfir innkominn tölvupóst, svarar símtölum og skrifar leiðbeiningar fyrir þá sem sent hafa inn beiðni um aðstoð eða eru í símanum. Tæknimenn GovCERT eru 7 talsins.

Hollenska stjórnsýslu-CSIRT teymið leggur mikla áherslu á virk og stöðug samskipti í samstarfsneti CSIRT og við aðra sem tengjast upplýsingaöryggi í landinu og á alþjóðavísu.

Meginstarf teymisins er söfnun upplýsinga úr ýmsum áttum, yfirferð þeirra, gerð leiðbeininga og útsending aðvarana um veikleika í tölvubúnaði, vírusa, orma og annað sem skiptir máli varðandi öryggi.

Upplýsingum er safnað bæði af opnum og lokuðum síðum á Netinu. Farið er yfir allar upplýsingaveitur á tveggja klst. fresti. Póstur af hverjum póstlista er skilgreindur í merktar möppur svo auðvelt sé að finna hann ef eitthvað fer úrskeiðis.

Til að fylgjast með vefsíðum er notaður vefsíðuvörður (websitewatcher), ódýrt forrit sem fer sjálfkrafa yfir bókamerki í vefsíðulistanum og merkir við þær sem hafa tekið breytingum. Þetta sparar mikinn tíma. Nokkur slík forrit standa til boða og sum eru "Open Source", þ.e. hægt að hlaða ókeypis niður af Netinu.

Eftirfarandi eru dæmigerð þrep sem teymið hefur tileinkað sér við meðhöndlun gagnaaðfanga:

- Mikilvægi metið.

[23] Unnið úr gögnum frá GovCERT

- Hvaðan eru upplýsingarnar? Er hægt að treysta upplýsingaveitunni og er hægt að staðfesta hvort þær eru réttar. Ákveðið ferli er notað til að athuga upplýsingar.
- Flokkun – Upplýsingar geta verið af ýmsum toga, bæði trúnaðarupplýsingar og opnar öllum. Reglur eru um hvernig fara skuli með mismunandi tegundir upplýsinga.
- Síun - GOVCERT.NL er með lista yfir allan hugbúnað og tölvur sem hagsmunaaðilar þeirra nota. Þannig getur teymið metið upplýsingar með tilliti til mikilvægis þeirra fyrir hagsmunaaðilana svo þeir fá einungis þær upplýsingar sem þeim henta.
- Miðlun upplýsinga inn á réttar boðleiðir.

GOVCERT.NL heldur úti virkri vefsíðu og sólarhringsþjónustu. Allar stofnanir og ráðuneyti innan stjórnsýslunnar geta gerst aðilar að GOVCERT.NL en ekki er skylduaðild. Þess vegna leggur GOVCERT.NL mikla áherslu á kynningar á mikilvægustu þáttunum í starfi sínu:

- Sólarhringsaðstoð.
- Sjálfstæð ráðgjöf.
- Ráðgjöfin sniðin að þörfum þiggjandans.
- Aðgerðir til að fyrirbyggja öryggisatvik.
- Viðbrögð við einstökum atvikum.
- Aðgengi að öðrum CSIRT á landsvísu og alþjóðavísu.

Viðskiptamenn GOVCERT.NL sem allir eru úr stjórnsýslustofnunum ríkisins í Hollandi þurfa ekki að greiða fyrir grunnþjónustu teymisins. Aðrir stjórnsýsluaðilar, svo sem sveitarstjórnir, vatnsveitur og aðrir þurfa að greiða félagsgjöld á kostnaðarverði.

Viðvaranir um vírusa og orma

GOVCERT.NL teymið í Hollandi hefur fengið góð viðbrögð við viðvörunum sínum, bæði við vírusum og ábendingar um veikleika. Áskrifendur að viðvörunum í tölvupósti voru orðnar 55.000 í júlí 2005.

Stuðningsupplýsingar og ráð um öryggi

GOVCERT.NL sendir frá sér mánaðarlegt fréttabréf þar sem gefið er yfirlit yfir þær viðvaranir sem sendar voru út mánuðinn á undan. Í fréttabréfinu eru einnig upplýsingar um það helsta sem er að gerast á þessu sviði á hverjum tíma. Teymið hefur fengið mjög góð viðbrögð við fréttabréfinu og í júlí 2005 voru áskriftir komnar yfir 16.000.

Árið 2005 voru leiðarljós GOVCERT stjórnsýslu-CSIRT teymisins í Hollandi:

- Að styðja og styrkja upplýsingaöryggi innan stjórnsýslunnar.
- Vakt allan sólarhringinn þar sem stjórnvöldum eru veittar upplýsingar, sendar viðvaranir og ráðgjöf veitt um hvers konar netvá.

- Vera miðpunktur þekkingar og upplýsingagjafar fyrir stjórnvöld.

Samkvæmt þessum leiðarljósum skyldi teymið:

- Vinna fyrir hollensk stjórnvöld í heild.
- Koma í veg fyrir öryggisatvik eins og hægt væri.
- Bregðast við atvikum.

Markmið og viðbrögð:

- Fyrsta markmið: Að koma í veg fyrir öryggisatvik á árangursríkan hátt.
    - Safna upplýsingum.
    - Miðla upplýsingum.
    - Miðla þekkingu.
    - Safna sérfræðiþekkingu.
    - Fá mismunandi aðila til samstarfs og samræðna til að deila upplýsingum.
    - Aðstoða önnur CSIRT teymi í samfélaginu.
    - Fylgjast með þróun og framvindu og greina áhættu.
    - Skipuleggja nám og fræðslumöguleika starfsmanna.

- Annað markmið: Árangursrík viðbrögð.
    - Skipulagning viðbragða við öryggisatvikum.
    - Verkfæri og verkferlar.
    - Spurningar um tækni og skipulag starfsemi (að þekkja viðskiptamannahópinn).
    - Öryggisskoðanir.

Leiðir GovCERT til fjármögnunar

Góð fjármögnun er grundvöllur árangurs af verkefninu. Ef verkefnisáætlunin er skýr og markviss auðveldar það fjármögnun. GOVCERT teymið í Hollandi gat strax hafið störf með krafti þar sem því voru tryggðir fjármunir frá upphafi. Teymið lagði mikla áherslu á að vinna að stefnumörkun með stjórnvöldum og senda reglulega frá sér skýrslur um gang verkefnisins. Þó slíkt sé mikil vinna styður hún starfið, hvetur starfsmenn til að endurskoða áfanga- og tímaáætlanir sínar reglulega og stuðlar að því að verkefnið sé unnið á ábyrgan og sjálfstæðan hátt.

Árlegt fjárframlag GOVCERT í Hollandi kemur frá innanríkisráðuneyti Hollands og Upplýsingaskrifstofu konungdæmisins.

- Fjármagn frá ríkisstjórninni til starfseminnar eru 2 milljónir evra.
- Aðrar stofnanir greiða kostnað samkvæmt gjaldskrá.
- Umbeðin aðstoð var seld út á kostnaðarverði. Sumir aðilar báðu um aukaráðgjöf og viðbótar öryggisathuganir. Gjald fyrir slíkt greiðir aukatíma og -vinnuframlag starfsmanna og veitir frelsi til að

útvega sérþekkingu eða mannafla til að sinna slíkum verkefnum. Þetta er nauðsynlegt þar sem starfsteymið er lítill.

Viðvörunarþjónusta fyrir almenning

Hollendingar ákváðu jafnframt að setja upp viðvörunarþjónustu - De Waarschuwingsdienst (www.waarschuwingsdienst.nl) - sem sinnir almenningi í Hollandi. Viðvörunarþjónustan er fjármögnuð af hollenska viðskiptaráðuneytinu.

Sú ímynd viðvörunarþjónustunnar sem GOVCERT.NL leggur áherslu á að koma til skila er tiltölulega einföld og samanstendur af eftirfarandi:

- Hluti stjórnsýslunnar
  Lögð var áhersla á að viðvörunarþjónustan væri á vegum stjórnvalda. Mikilvægt er að ljóst sé að þjónustan eigi ekki markaðshagsmuna að gæta.

- Sjálfstæði
  Viðvörunarþjónustan sé sjálfstæð og allar upplýsingar frá henni byggist á staðreyndum eða mati sérfræðinga. Ekki sé neinn dulinn tilgangur eða áhrif frá þeim markaðsaðilum sem þjónustan er í sambandi við.

- Skjótvirkni
  Til þess að viðvörunarþjónusta öðlist traust þarf hún að sýna skjót viðbrögð. Þetta þýðir ekki endilega að vera alltaf fyrst með allar upplýsingar því gæði upplýsinganna eru ætíð í fyrsta sæti.

- Áreiðanleiki
  Annað mikilvægt atriði til að byggja upp traust og trúverðugleika er áreiðanleiki. Fólk reiðir sig á upplýsingar frá þjónustunni. Eins og kom fram hér á undan þýðir það að vera áreiðanlegur að ekki er alltaf hægt að koma fyrst fram með upplýsingarnar. Þetta þýðir að alltaf er hægt að treysta upplýsingum sem sendar eru út.

- Ókeypis þjónusta
  Ábyrgðaraðilar viðvörunarþjónustu GOVCERT.NL í Hollandi ákváðu að hún skyldi vera ókeypis.

Í upphafi setti viðvörunarþjónusta GOVCERT.NL ekki upp fyrirfram ákveðnar aðferðir til að koma skilaboðum sínum áfram í gegnum útvarp. Eftir að þjónustan hafði starfað í eitt ár hafði ríkisútvarpið í Hollandi samband og bað um að þjónustan kæmi inn með fregnir af viðvörunum daginn eftir að þær væru sendar út á póstlista þjónustunnar.

Eftir að hafa fengið ábendingar frá hagsmunaaðilum sínum setti hollenska viðvörunarþjónustan upp möguleika á RSS streymi á fréttasíðu sinni. Allmargir hafa nýtt sér þennan möguleika.

21 VIÐAUKI E - VIÐVÖRUNARHÓPAR (WARP)

WARP hópar (Warnings, Advice and Reporting Point) eiga upptök sín á Bretlandseyjum og er starfsemi þeirra að mestu leyti bundin við viðvörunarþjónustu. Hér verður minnst á þá sem valkost, enda er hugur í þeim að útvíkka starfsemina til annarra landa og eru þeir nú þegar komnir til Belgíu og Hollands. Forvígisstofnunin í Bretlandi er CPNI (Center for the Protection of National Infrastructure), þ.e sú stofnun sem fer með vernd innviða á landsvísu. Sérhver WARP hópur samanstendur af WARP veitu (WARP provider), sem sér um rekstur daglegrar WARP þjónustu og WARP meðlimum (WARP peers) sem fá valin gögn frá WARP veitunni gegnum WARP samskiptahugbúnað (WARP Filtered Warning Application Software) veitunnar. Sérhver WARP veita og meðlimir hennar, setja sér ákveðin mörk um hverju þau miðla innan teymisins, svo sem um málefni tiltekins netbúnaðar. WARP meðlimir geta verið fjarskiptafyrirtæki og/eða einstaklingar innan hvers þeirra. WARP veitur eru hluti af samfélagi, sem miðlar á milli sín ráðleggingum um bestu tæknilegu leiðir, ásamt fyrirséðum ógnum og öryggisatvikum, á sem ódýrastan hátt. Miðlunin fer yfirleitt fram annað hvort á rafrænum umræðufundum eða gegnum fyrrgreindan WARP samskiptahugbúnað. Samskiptahugbúnaðurinn er ennfremur útbúinn síunarkerfi (filtering system) sem veiturnar nota til að miðla til meðlima sinna, eða annarra WARP veitna, gögnum sem henta þeim í hvert sinn. WARP veitan þarf að uppfylla viss atriði í ISO 27001 staðlinum sem erfist til meðlima hennar. Hún er yfirleitt mönnuð með einum kerfisstjóra og einum minna tæknimenntuðum starfsmanni, báðir í fullu starfi. Að auki þarf að koma til aðkeypt sérfræðiaðstoð, ef svo ber undir. WARP meðlimur þarf aftur á móti vaktmann og samskiptahugbúnað. Engin skipulögð rannsóknarstarfsemi fer fram innan WARP samfélagsins, heldur eingöngu miðlun upplýsinga byggð á reynslu, svo sem af samvinnu við framleiðendur búnaðar. Meðlimir geta líka miðlað upplýsingum á milli sín, undir nafni eða nafnlaust. Ef einn meðlimur kemst að raun um t.d. óvæntan galla í hugbúnaði, miðlar hann þeim upplýsingum til annarra meðlima innan teymisins. Meðlimurinn getur síðan fengið úrlausn frá framleiðanda hugbúnaðarins og lætur þá aðra meðlimi vita. Dæmi eru um að meðlimirnir miðli sinni reynslu á milli sín um hvort óhætt er að innleiða nýjar stigbætur/endurbætur (update) ákveðins hugbúnaðar. WARP veitan ákveður hvort miðla skuli þessum upplýsingum frekar innan WARP samfélagsins með ofangreindum leiðum. Enn sem komið er eru þessir viðvörunarhópar nær eingöngu svæðisbundið á Bretlandseyjum og einn hópur er í Hollandi og annar í Belgíu. ENISA bendir á að þeir gætu hentað sem milliskref áður en fjarskiptafyrirtæki og aðrir aðilar stofni sinn „innri CSIRT“, en í sömu andrá segja þeir æskilegra að stefna strax alla leið.

Skv. WARP (www.warp.gov.uk) í Bretlandi má reikna með stofnkostnaði WARP veitu í kringum hálfa milljón fyrsta árið vegna kaupa á tölvubúnaði og öryggisvörnum, uppsetningar sérstaks samskiptavefs o.s.frv. Ennfremur megi reikna með árlegum rekstrarkostnaði veitunnar að lágmarki í kringum 6-7 milljónir kr., þar sem laun 2ja starfsmanna og aðkeypt aðstoð vega mest. Hluti rekstrarkostnaðarins dreifist á WARP meðlimi sem þar að auki þurfa að útvega vaktmann hjá sér. Miðað við íslenskar aðstæður má gera ráð fyrir að allur fyrrgreindur kostnaður sé varlega áætlaður.

Samanburður á WARP og CSIRT

Fullvaxin CSIRT eru algengari en WARP hópar. Þau stunda öflugri starfsemi, svo sem rannsóknarvinnu, og eiga kost á víðtækari samskiptum á heimsvísu sín á milli. Þau eru því betur í stakk búnir að bregðast við og veita viðskiptamönnum sínum ráðleggingar gegn hvers konar netvá. Í fljótu bragði má segja að hlutverk WARP hópa sé að koma í veg fyrir að öryggisbrestir eigi sér stað, en CSIRT að minnka áhrif brestanna. WARP hópar starfa í umboði tiltekins smærri hóps hagsmunaaðila og þeir sérhæfa sig í samræmi. Þ.e.a.s.

hver viðvörunarhópur þjónar yfirleitt mun færri hagsmunaaðilum en CSIRT, eða á bilinu 20-100, og er verksvið þeirra oft þrengra, t.d. umræður um tiltekinn búnað.

Í stuttu mál henta viðvörunarhópar síður til stærri verkefna og stendur þjóðar-CSIRT þeim framar til úrlausnar verkefna á landsvísu.

Niðurstaða skýrsluhöfunda er því sú að fremur skuli stefna að stofnun þjóðar-CSIRT teymis til að berjast við vaxandi öryggisógnir í fjarskipta- og upplýsinganetum. Æskilegast er að slík forystuteymi stuðli bæði að vernd Internetsins á Íslandi, svo og annarra mikilvægra innviða í fjarskipta- og upplýsinganetum.