Efnisyfirlit

Frá hópstjóra sveitarinnar

Netöryggissveitin CERT-ÍS er fyrsta netöryggissveitin á Íslandi sem starfar á landvísu (e. National CERT). Sveitin var stofnuð fyrir tilstuðlan Ögmundar Jónassonar innanríkisráðherra (þá samgönguráðherra) með bréfi dagsettu 4. nóvember 2011. Var ákveðið að hún yrði starfrækt innan Póst- og fjarskiptastofnunar. Má með sanni segja að ekki hafi verið átakalaust koma sveitinni á fót, enda hafði umræða og undirbúningur að stofnun slíkrar sveitar staðið yfir allt frá árinu 2008. Í framhaldi af bréfi innanríkisráðherra haustið 2011 samþykkti Alþingi breytingu á fjarskiptalögum vorið 2012 þar sem ákvæði um sveitina voru sett í lög. Reglugerð um starfsemina tók svo gildi þann 1. júní 2013. Í framhaldi af því hóf sveitin formlega störf.

Er þetta fyrsta ársskýrslan sem netöryggissveitin CERT-ÍS sendir frá sér. Henni er ætlað að veita innsýn í starfsemi og viðfangsefni sveitarinnar. Hugtakið netöryggissveit er þýðing á hinu enska heiti Computer Emergency Response Team (skammstafað CERT).

Markmið CERT-ÍS eru að fyrirbyggja, draga úr og bregðast við hættu vegna netárása eða hliðstæðra öryggisatvika í þeim tölvukerfum sem falla undir starfssvið sveitarinnar, þ.e. í netumdæmi hennar. Sveitin veitir hlutaðeigandi stuðning, t.d. með því að greina öryggisatvik, aðstoða við að takmarka útbreiðslu þeirra og minnka á annan hátt tjón af þeirra völdum. Við útbreidd og alvarleg öryggisatvik samhæfir sveitin viðbrögð og aðgerðir. Sem dæmi má nefna að ef neyðarástand skapast í netheimum, sinnir sveitin samhæfingar- og samræmingarhlutverki innan netumdæmisins með markvissum upplýsingaskiptum og neyðarsamráði. Er þetta verkefni falið sveitinni á þeim forsendum að hún sé óháður aðili og geti starfað með því trausti sem nauðsynlegt er. Slík samvinna er fastmótuð í samstarfi við aðila þjónustuhópsins með tilliti til skipulags, undirbúnings og aðstöðu.

Þjónusta sveitarinnar snýr í dag fyrst og fremst að fjarskiptafyrirtækjum. Einnig er sveitinni heimilt að gera sérstakan þjónustusamning við þá aðila sem reka ómissandi upplýsingainnviði . Ómissandi upplýsingainnviðir þessara aðila mynda svokallað netumdæmi sveitarinnar. Þar er eingöngu átt við hina tæknilegu innviði þjónustuhópsins. Til hliðar við kjarnaþjónustu sína veitir sveitin tiltekna þjónustu fyrir allt landið, svokallaða landsþjónustu. (*Sjá nánari þjónustulýsingu á bls. 8*).

Þótt starfsemi netöryggissveitarinnar hafi hafist á árinu 2013 er ljóst að nauðsynlegt er að styrkja hana töluvert svo hún geti uppfyllt grunnþarfir þjóðfélagsins. M.a. þarf að stækka þjónustuhóp hennar umtalsvert. Má leiða að því líkur að skynsamlegast sé fyrir Ísland, sem lítið og fámennt land, að byggja upp eina sterka netöryggissveit, frekar en dreifa þekkingu og ábyrgð starfseminnar milli ýmissa aðila. Þar ber að hafa í huga að fjöldi þeirra sem hafa næga menntun á sviði netöryggis er takmarkaður hérlendis og ein vel mönnuð sveit með vítt umdæmi er betur til þess fallin en margar minni sveitir að ná þeim markmiðum sem sett eru, t.d. er snýr að þjónustutíma og þekkingaröflun. Slíkt fyrirkomulag yki einnig möguleika til að mynda sérþekkingu á einstaka geirum þjóðfélagsins og sérhæfðri samvinnu við þá. Ljóst er þó að fyrirtæki innan einstaka geira verða að vinna náið saman að netöryggismálum til að árangur náist.

Árið 2013 var viðburðarríkt þegar litið er til netöryggismála. Sveitin vann að tveimur málum sem flokkast sem alvarleg. Annars vegar var um að ræða netárás á Vodafone og hins vegar meintan umferðarstuld sem tengdist Símanum hf. en fjallað er stuttlega um bæði málin síðar í skýrslunni.

Töluverður fjöldi minni mála komu einnig til meðferðar hjá netöryggissveitinni á árinu. Ekki verður nánar gert grein fyrir þeim hér, en þau koma fram í tölfræði um starfsemina.

Stöðugt koma fram nýjar ógnir og upplýsingar sem valda óróa varðandi netöryggi. Sumt af því nýjasta kemur til vegna uppljóstrana á upplýsingum og annað vegna mikils hraða í þróun tækninýjunga. Á hverjum tíma er nauðsynlegt að takast á við aðsteðjandi hættur með þekkingu á nýjustu tækniþróun og aðferðum tölvuþrjóta. CERT-ÍS er því mikilvægur þáttur í heildar netöryggisviðbúnaði hérlendis. Flest þau einkafyrirtæki sem koma að þessum málum gera það til að tryggja sem best eigin rekstur og öryggi viðskiptavina sinna. Það er hins vegar á hendi opinberra aðila og stjórnvalda á hverjum tíma að hafa umsjón með stefnumótun, lagasetningu og eftirliti með tilliti til öryggis samfélagsins alls og ljóst er að mikið verk er þar óunnið.

Stefnt er að því að stækka þjónustuhóp sveitarinnar þannig að starfsemi hennar nái einnig til fyrirtækja og stofnana utan fjarskiptamarkaðarins, svo sem í orku- og fjármálageiranum. Þessir geirar eru lykilgeirar fyrir þjóðfélagið og mega síst við því að verða óstarfhæfir eða verða fyrir öðrum alvarlegum truflunum af völdum netöryggisatvika, jafnvel í stuttan tíma. Er því mikil þörf á að vernda upplýsingainnviði þeirra og rætt er um þessa innviði sem ómissandi upplýsingainnviði Íslands (e. Critical Information Infrastructure, CII).

Á verkefnasviðinu verður á árinu 2014 lögð áhersla á endurbætt upplýsingaskiptakerfi sveitarinnar, þátttöku í sameiginlegum æfingum, sem og samhæfingu og samræmingu viðbragða við stóráföllum. Ekki síst verður lögð vinna í uppbyggingu á ástandssetri sveitarinnar (e. Situation Awareness Centre), þ.e. nokkurs konar upplýsinga- og stjórnstöðvar sem verður virkjuð meðan tiltekið ástand varir sem veldur eða getur valdið ógn. Einnig er stefnt að að CERT-ÍS muni tengjast samnorrænu upplýsingaskiptaneti norrænna netöryggissveita.

Ljóst er að vitund um netöryggismál og viðbúnaður gagnvart ógnum í upplýsingainnviðum er að eflast í íslensku samfélagi. Allt er það í rétta átt og því er óhætt fyrir starfsmenn netöryggissveitarinnar CERT-ÍS að líta björtum augum til framtíðar og takast með tilhlökkun á við ný verkefni á komandi árum.

Stefán Snorri Stefánsson

Hópstjóri CERT-ÍS netöryggissveitarinnar

Yfirlit 2013

Í júní 2013, með gildistöku reglugerðar um netöryggissveitina, hófst starfsemi hennar með formlegum hætti. Þar með var hægt að ljúka við skilgreiningu á þjónustu sveitarinnar, en formleg þjónustulýsing sveitarinnar leit dagsins ljós í lok ársins. Er umfjöllun um hana síðar í skýrslunni.

Daglegur rekstur

Daglega kemur mikill fjöldi minniháttar mála inn á borð netöryggissveita um allan heim, þ.e. minni öryggisatvik sem unnið er úr með þeim sem fyrir þeim verða. Þegar litið er til CERT-ÍS er oftast um að ræða veikleika í rekstri tölvukerfa og er þá upplýsingum komið áleiðis til viðeigandi kerfisstjóra eða netrekanda. Einnig berst töluvert af tilkynningum um að árás hafi verið gerð frá íslensku neti. Yfirleitt er þá um að ræða vélar sem sýktar eru af óværum og er fjarstýrt af óprúttnum aðilum t.d. til netárása.

Á árinu kom töluverður fjöldi atvika til kasta sveitarinnar þar sem verið var að misnota veikleika í þekktum vefumsjónarkerfum. Eru kerfisstjórar hvattir til að fylgjast vel með uppfærslum á slíkum hugbúnaði og þá sérstaklega viðbótum (e. plugins/extensions).

Sveitin er einnig þjónustuhópnum innan handar með ráðleggingar varðandi netöryggi sem og upplýsingamiðlun innan þjónustuhópsins. Komi þannig upp spurningar, til að mynda um hvort atvik séu útbreidd til annarra fyrirtækja, berast fyrirspurnir til sveitarinnar sem getur þá grennslast fyrir og komið málum í rétt ferli sé um slíkt að ræða.

Stærri öryggisatvik komu einnig inn á borð sveitarinnar á árinu 2013. Tekið var á þeim eftir viðeigandi ferlum en ekki rata öll þeirra í opinbera umræðu af ýmsum ástæðum. Tvö atvik ársins gerðu það hins vegar og er farið yfir þau sérstaklega hér á eftir.

Kerfi til upplýsingamiðlunar

Ein meginstoðin í starfsemi netöryggissveitarinnar er miðlun upplýsinga um netöryggisatvik til ábyrgðaraðila neta. Á árinu var unnið að innleiðingu sjálfvirks kerfis til að annast þessa upplýsingamiðlun. Upplýsingar sem miðlað er í gegnum kerfið eru fyrst og fremst tilkynningar frá ytri aðilum um að eitthvað óeðlilegt hafi sést frá vélum staðsettum á Íslandi og biður tilkynnandinn um að viðkomandi ábyrgðaraðila sé gert viðvart þannig að bregðast megi við. Slík tilkynning er móttekin og flokkuð, bæði með tilliti til móttakanda og eðlis atviks. Þannig geta móttakendur forgangsraðað viðbrögðum út frá efni tilkynningarinnar, þ.e. hvort hún snýst um ruslpóst, óværu, tilraun til þjónusturofs (e. denial of service attack) eða annað. Slíkum tilkynningum er komið áfram til þeirra aðila sem hafa fengið úthlutaðri viðkomandi IP tölu frá RIPE NCC (Réseaux IP Européens Network Coordination Center) og eru þannig ábyrgðaraðilar hennar. CERT-ÍS hefur samkvæmt lögum ekki heimild til að nálgast upplýsingar um viðskiptavini fjarskiptafyrirtækja, og því er það í höndum hvers fyrirtækis að sjá um að tilkynningin komist til skila.

Fyrstu prófanir á kerfinu hafa verið jákvæðar og er notkun þess mikill styrkur fyrir netöryggissveitina, þar sem sjálfvirkni og sjálfsafgreiðsla eru mikilvægir þættir. Jafnframt er

verið að byggja upp þjónustuvef á www.cert.is fyrir þá aðila sem sveitin sinnir og unnið er að því að samþætta sjálfvirka upplýsingamiðlunarkerfið við þann þjónustuvef. Stefnt er á að þjónustuvefurinn opni formlega á árinu 2014.

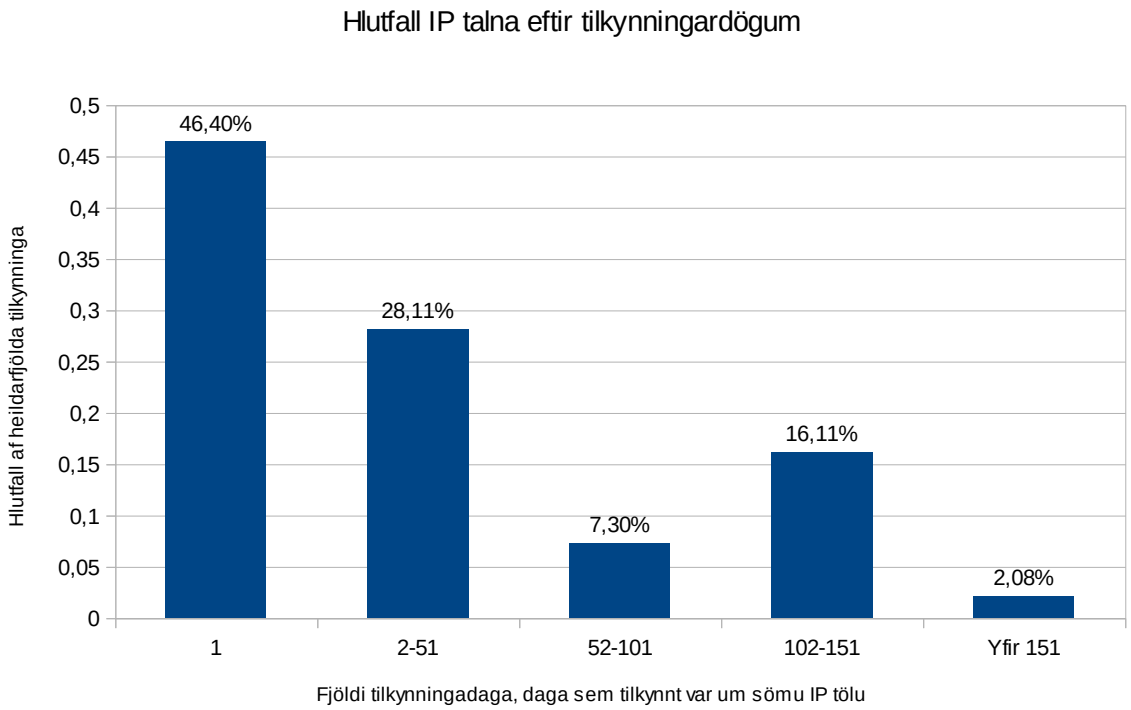
Lykiltölur um upplýsingamiðlun

CERT-ÍS viðheldur á hverjum tíma ástandsmynd af netöryggisatvikum, stórum sem smáum, á íslenska netinu. Uppistaðan í þeirri mynd eru tilkynningar annars staðar úr netinu um að óæskileg umferð hafi borist frá Íslandi. Slíkar tilkynningar eru því vísbendingar um að eitthvað sé að tölvum á Íslandi, að þær hafi verið sýktar af óværum, brotist inn á þær, eða hægt að misnota þær á annan hátt.

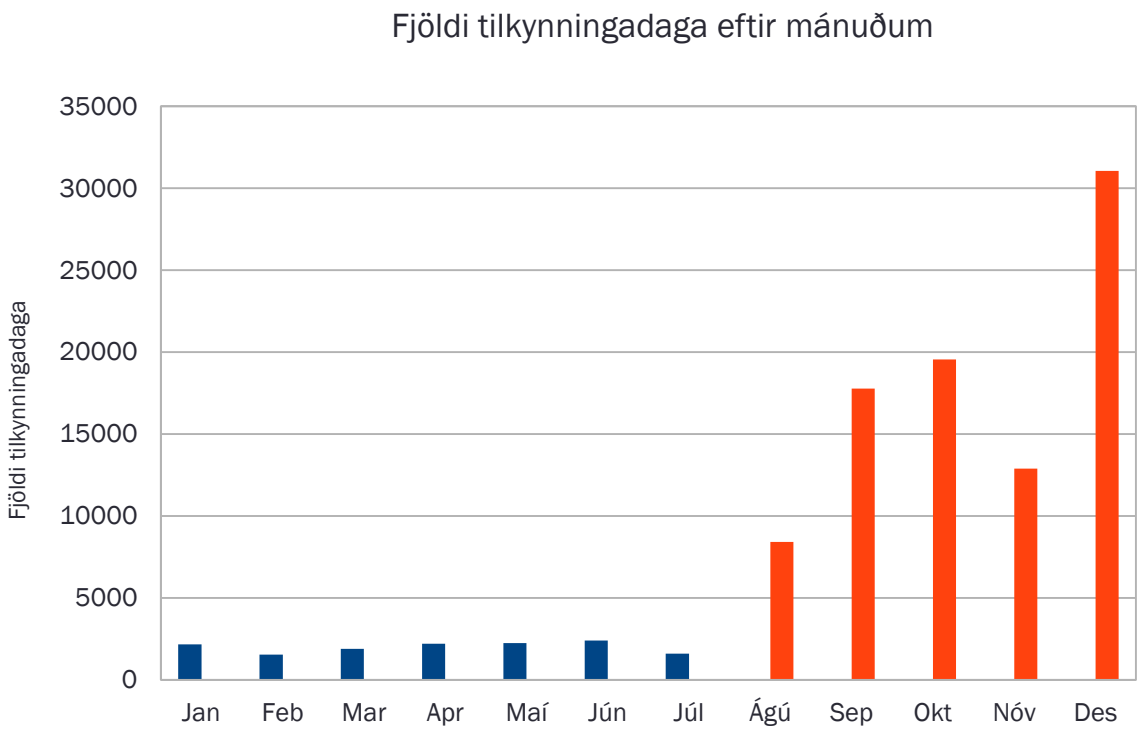
Öllum tölum sem hér koma fram ber að taka með fyrirvara, tilkynningar geta verið ónákvæmar þar sem þær eru ekki staðfestar, þær geta átt við sömu vélina þótt IP talan sé önnur, þær geta átt við mismunandi vélar þótt IP talan sé sú sama, og þetta er aðeins hluti af heildarmyndinni. Einnig ber að hafa í huga að tilkynningar geta verið misalvarlegar.

Árið 2013 var tilkynnt um 10.509 IP tölur sem netinu hérlendis stafaði ógn af á mismunandi hátt. Af þeim voru 4.876 IP tölur þar sem tilkynningar stóðu aðeins yfir í einn dag eða skemur. Fjöldi IP talna þar sem tilkynningar um sömu IP töluna stóðu yfir í fimm eða færri daga var 5.697. Af þessu má greina að u.þ.b. helmingur allra vandamála er leystur fljótt.

CERT-ÍS tók sérstaklega á 14 málum á árinu, en það voru mál sem voru aðkallandi með einum eða öðrum hætti.

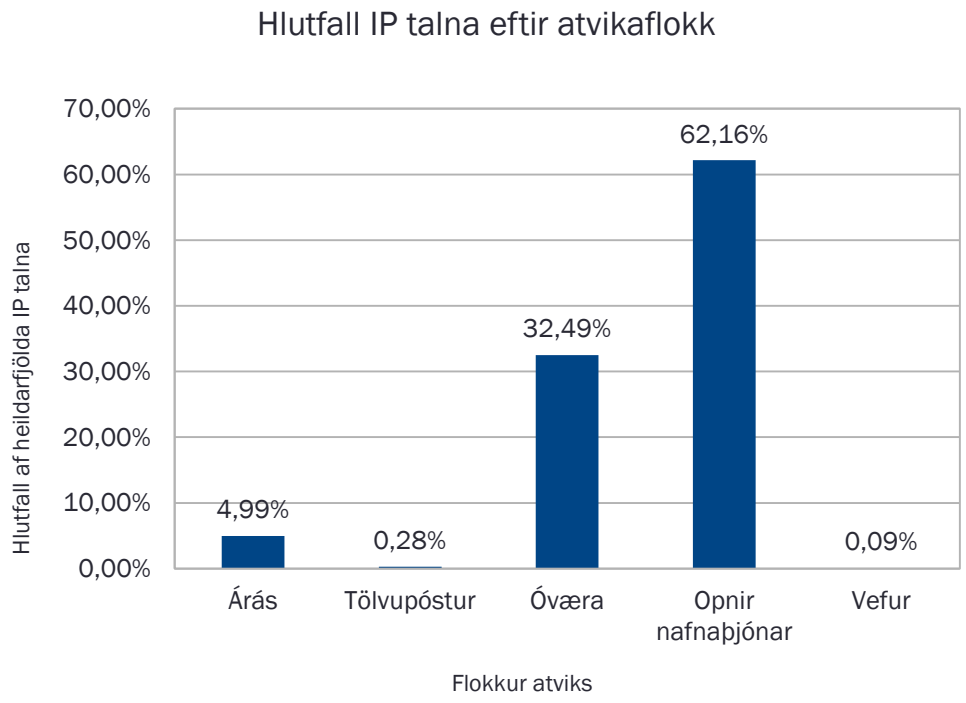


Stöðugt er unnið í að fá betri mynd af ástandinu og má sjá að þegar fleiri gagnalindir bættust inn í byrjun hausts 2013 jókst fjöldi tilkynninga sem sveitin fékk töluvert.



Atvik sem tilkynnt er um eru mjög mismunandi, en skiptingu þeirra í helstu flokka yfir árið má sjá á mynd 1. Athygli vekur að mikið hefur borist af tilkynningum um rangt stillta nafnaþjóna.

Mynd 1.



Stefnumótunarvinna

Fyrir hönd sveitarinnar er hópstjóri hennar þátttakandi í vinnuhóp innanríkisráðuneytisins um mótun stefnu Íslands í netöryggi. Aðal verkefni hópsins er að móta stefnu stjórnvalda um net- og upplýsingaöryggi og vernd upplýsingainnviða er varða þjóðaröryggi. Í starfshópnum sitja fulltrúar innanríkisráðuneytis, Ríkislögreglustjóra, Póst- og fjarskiptastofnunar og utanríkisráðuneytisins. Nánari upplýsingar um hlutverk og starf hópsins er að finna á vef innanríkisráðuneytisins.

Æfingar og þjálfun

Æfingar hafa til þessa reynst vel til þess að samræma viðbrögð og ferla, sem og efla tengsl aðila á markaði.

Þetta á við um netöryggismál eins og önnur öryggismál. Því er mikilvægt að stærri þjónustuaðilar snúi bökum saman og æfi sig saman í að verjast þeim netógnum sem steðja að í netheimum nútímans. Í því samhengi er líka áríðandi að allir þeir sem hafa mikilvægu hlutverki að gegna þegar áföll ríða yfir, æfi saman og þjálfi samstillt viðbrögð gagnvart stærri ógnum.

Munu slíkar æfingar sem og æfingar þar sem líkt er eftir raunverulegum atburðum verða reglulegur þáttur í starfsemi sveitarinnar.

Netútlaginn

Í nóvember var haldin fyrsta eiginlega netvarnaræfingin hérlendis undir stjórn CERT-ÍS, og gekk hún undir nafninu Netútlaginn 2013. Að þessu sinni var einungis stærri aðilum þjónustuhópsins, sem veita öðrum ómissandi upplýsingainnviðum þjónustu, boðin þátttaka. Æfingin var svokölluð skrifborðsæfing (e. Tabletop Exercise), þar sem þátttakendur og skipuleggjendur sitja allir í sama herbergi. Sá netöryggissveitin um undirbúning æfingarinnar og utanumhald með innleggi frá þátttakendum. Farið var í gegnum ímyndaðar atburðarásir og skoðað hvaða viðbrögð væru viðhöfð. Eftir æfinguna var svo farið með þátttakendum yfir heildarmyndina, hvað reyndist vel og hvar mætti bæta úr. Ein helsta niðurstaða æfingarinnar var sú hversu mikilvægt er að tilkynna grunsamleg atvik til CERT-ÍS strax á fyrstu stigum. Með slíkri upplýsingagjöf fæst heildarmynd af atburðarás sem getur hugsanlega verið í gangi samtímis hjá öðrum aðilum netumdæmisins og því hægt að samstilla krafta allra viðkomandi aðila. Þau persónulegu tengsl sem myndast á æfingum sem þessum eru mjög mikilvæg við að brjóta niður múra og koma í veg fyrir samskiptaörðugleika.

Undirbúningur samevrópskrar netvarnaræfingar, Cyber Europe 2014

Á árinu 2014 verður haldin samevrópsk netvarnaræfing ESB/ESS þjóða, með þátttöku netöryggissveita, einkaaðila og opinberra stofnana, og mun CERT-ÍS taka þátt í æfingunni ásamt öðrum íslenskum aðilum. Áhersla æfingarinnar er raforkugeirinn, og munu verkefni hennar því verða stíluð að vissu leyti inn á það. Þátttaka í æfingum skilar bestum árangri þegar er tekinn virkur þáttur í undirbúningi hennar og hefur CERT-ÍS tekið þátt í þeim fundum frá upphafi. Áður hefur Póst- og fjarskiptastofnun tvisvar tekið þátt í samevrópskum netvarnaræfingum, árið 2010 sem áhorfandi og svo 2012 sem virkur þátttakandi ásamt tveimur öðrum íslenskum aðilum.

Starfsemi sveitarinnar

Starfsemi og þjónusta CERT netöryggissveita snýst ekki um bein inngrip með aðgerðum á netkerfi og þjónustu þeirra sem sveitin þjónar, heldur er um að ræða tilmæli og ráðgjöf varðandi viðbrögð, bæði á sviði fyrirbyggjandi skipulags og hvað beri að gera þegar öryggisatvik koma upp. Þjónustan skiptist í höfuðdráttum í tvennt; svokallaða kjarnaþjónustu og þjónustu á landsvísu. Hér verður drepið á þjónustulýsingu sveitarinnar eins og hún var 10. janúar 2014 og gefin nánari útskýring og markmið. Þjónustulýsingin getur tekið breytingum en gildandi lýsingu á hverjum tíma má finna á vefsíðu sveitarinnar (www.cert.is).

Þjónustulýsing

Kjarnaþjónusta

Eftirtalin þjónusta er aðeins ætluð aðilum þjónustuhópsins og myndar grunn netöryggissveitarinnar.

1. Meðferð vegna öryggisatvika

Sveitin ráðleggur og/eða aðstoðar við að hrinda ákveðnum viðbrögðum af stað innan netumdæmisins, samræmir aðgerðir sé þess þörf og metur hvort gera þarf öðrum viðvart um atvikið.

Markmiðið með þessum hluta starfseminnar er að draga úr eða koma í veg fyrir tjón af völdum öryggisatvika. Komi upp öryggisatvik getur viðkomandi aðili óskað eftir aðkomu netöryggissveitarinnar. Fer slík aðstoð eftir aðstæðum og óskum í hvert sinn. Sömuleiðis getur sveitin tilkynnt hlutaðeigandi þjónustuveitanda um yfirvofandi ógn eða öryggisatvik, sem gæti stofnað tæknilegum rekstri hans í hættu og óskað eftir tilteknum viðbrögðum af hans hálfu.

Sjálf meðferðin vegna öryggisatvika felur í sér fastmótað verklagsferli, sem yfirleitt hefst á því að vaktmaður sveitarinnar hverju sinni frumskoðar öryggisatvikið og metur þörf á viðbrögðum. Ef hætta er á ferðum er forgangur atviksins metinn, og það svo meðhöndlað með nánari greiningu m.t.t. yfirvofandi ógnar og mögulegum áhrifum hennar. Oftar en ekki lýkur atvikum með ráðleggingum til hlutaðeigandi aðila um viðeigandi viðbrögð gegn ógninni hverju sinni, upplýsingamiðlun eða beiðni um viðbrögð annarra aðila. Ef um er að ræða útbreitt atvik eða sérstaka hættu er lýst yfir viðbúnaðarstigi hjá sveitinni og samræming aðgerða á víðari grundvelli tekur við.

2. Fastmótuð samræming og samhæfing

Í neyðarástandi sinnir sveitin samhæfingar- og samræmingarhlutverki innan netumdæmisins. Slík samvinna er fastmótuð með aðilum þjónustuhópsins sem og almannavarnaraðilum með tilliti til skipulags, undirbúnings og aðstöðu. Nauðsynlegar heimildir til ákvarðanatöku og aðgerða eru fyrirfram skilgreindar.

Samráðsvettvangur er myndaður um tiltekin málefni og/eða innan þess geira þjóðfélagsins sem viðkomandi aðili er í.

Markmiðið með þessu er að samræma og stjórna neyðaraðgerðum eins og kostur er, þegar stóráföll í netheimum dynja yfir. Hér eiga aðallega þeir í hlut sem eru hluti af umdæmi

sveitarinnar sem jafnframt er nokkurs konar „neyðar“-umdæmi hennar. Viðkomandi aðilar taka með netöryggissveitinni þátt í að móta ákveðið verklag við samhæfingu. Viðbragðsáætlanir eru samstilltar ásamt viðeigandi verkferlum og stjórnkerfi.

Fundir samráðsvettvangs aðila í sama geira eru haldnir reglulega til að ræða veikleika og ógnir, skoða hvað megi bæta, þróa samstarfið enn frekar, mynda styrkari tengsl milli aðila, gera áætlanir á þessu sviði og fleira.

Inn í fastmótað samstarf á þessu sviði tengjast netæfingar og þjálfun, sem og stefnumótuð ástandsvitund á hverju augnabliki og markviss upplýsingaskipti að hluta til.

3. Netæfingar og þjálfun

Sveitin stendur fyrir og/eða tekur þátt í netvarnar- og þanþolsæfingum (Cyber Exercises) sem fyrst og fremst snúa að netumdæminu. Áhersla í æfingum er breytileg, sem og hverjir innan netumdæmisins taka þátt hverju sinni. Æfingar geta verið alþjóðlegar eða bundnar við Ísland og taka yfirleitt mið af sviðsettu neyðarástandi í netheimum.

Markmiðið hér er að þróa enn frekar samstarf, viðbrögð, skipulag og verklag við stóráföllum með sameiginlegum netvarnaræfingum á vegum CERT-ÍS. Á sviði netöryggis skila æfingarnar almennt aukinni reynslu, betri og markvissari viðbúnaði og meiri samheldni þeirra sem taka þátt í þeim. Allt kemur það að góðum notum þegar tekist er á við raunveruleg áföll.

4. Upplýsingaskipti

Öllum aðilum í þjónustuhópnum er jafnóðum haldið upplýstum um það ástand sem kemur fram við gagnaöflun. Á þjónustuvef fá skráðir aðilar innan þjónustuhópsins tilkynningar um þau atvik sem snúa að þeim og þar geta þeir jafnframt sent inn tilkynningar um það sem þeir verða áskynja um í sínum innviðum.

Markmiðið með þessu er að afla vitneskju um almennt ástand netöryggis og kalla fram skjót viðbrögð hlutaðeigandi. Netöryggissveitin CERT-ÍS og þjónustuaðilar hennar skiptast sömuleiðis á gagnlegum upplýsingum um aðsteðjandi ógnir, öryggisatvik og annað.

5. Ástandsvitund

Í samvinnu við þjónustuhópinn vinnur sveitin að því að efla sem best ástandsvitund (Situation Awareness), þar sem fylgst er náið með viðbúnaði og ástandi innviða netumdæmisins frá degi til dags. Heildarmynd af ástandi netöryggismála innan netumdæmisins má fá með því að meta fyrirfram áhrif mismunandi öryggisatvika og stóráfalla. Tilgangurinn er að stuðla að réttri ákvarðanatöku þegar á reynir, svo og að virkja nauðsynlegar viðbragðsáætlanir tímanlega.

Markmiðið með þessu er að efla vitneskju um sem flesta þætti ríkjandi ástands hverju sinni sérstaklega við stóráföll en líka þess utan. Stefnt er að því að netöryggissveitin viðhaldi þekkingu á ástandi og stöðu innan og utan umdæmi síns á hverjum tíma og nýti hana til gerðar áhættulíkans á landsvísu. Með því verður ákvarðanataka í stóráföllum og í viðbúnaði

markvissari. Aðilar munu taka þátt í þessari samvinnu með því að veita sveitinni nauðsynlegar upplýsingar í þessum tilgangi.

Landsþjónusta

Taka skal fram að landsþjónustan er ekki kjarnaþjónusta hópsins, þ.e. ekki í fyrsta forgangi, heldur styður hún við öryggismál í netumdæminu, jafnframt því að efla almennt netöryggi innanlands.

1. Landstengiliður

CERT-ÍS er landstengiliður fyrir Ísland (e. National Point of Contact) um CERT-málefni. Þetta þýðir að sveitin vísar upplýsingum og fyrirspurnum sem henni hafa borist um öryggisatvik til hlutaðeigandi aðila hérlendis og erlendis eftir því sem eðli mála gefur tilefni til. Sveitin heldur utan um tengiliða- og þjónustuskrá.

Markmiðið hér er að einfalda samvinnu og samskipti innanlands og við útlönd, með því að sveitin hafi heildaryfirlit um stöðu mála. Í þessum tilgangi er sveitin sá milligönguaðili hérlendis sem leita skal til þegar ekki er ljóst hver sinnir tilteknu erindi sem snýr að netöryggisógnum, eða þau erindi sem send hafa verið öðrum aðilum þokast ekki áfram. Oft kemur fyrir að aðilar senda afrit á sveitina þegar þeir óska eftir að erindi sitt sé fylgt eftir af hendi annars rekstraraðila, eða til að leggja áherslu á mikilvægi málsins. Sveitin fylgist á þann hátt með framgangi mála en grípur ekki inn í nema sérstaklega sé þörf á. Sveitin er þannig sá aðili hérlendis sem ber ábyrgð á að samskipti innanlands og við útlönd er varða CERT-málefni Íslands gangi fljótt og vel fyrir sig. Ennfremur er inni í þessu hlutverki það verkefni að vera miðpunktur hérlendis um sömu mál, m.a. er varðar þátttöku í alþjóðlegum netöryggisæfingum.

2. Samráðsvettvangur innanlands

Sveitin tekur þátt í almennri umræðu um netöryggismál m.a. með þátttöku í eða skipan samráðsvettvangs um ýmis tæknileg viðbrögð og skipulag vegna öryggisatvika hérlendis.

Markmiðið hér er að efla umræðuvettvang hérlendis með beinni og óbeinni aðkomu sveitarinnar, þar sem rætt er um málefni tengd netöryggi almennt sem og mál sem varða ómissandi upplýsingainnviði. Ennfremur að koma á samráðsvettvangi um tiltekin málefni sem eru brennandi hverju sinni, t.d. sameiginleg varnarviðbrögð og forvarnir.

3. Ráðgjöf og leiðbeiningar

Sveitin veitir almenna ráðgjöf um aðgerðir og viðbúnað þegar svo ber undir. Þetta á einnig við um ráðgjöf varðandi undirbúning og uppsetningu á öðrum netöryggissveitum hérlendis.

Sveitin gefur út leiðbeiningar í tengslum við alvarleg öryggisatvik sem hætta er á að breiðist út til netumdæmisins, eða ef atvik eða ástand varðar stóran hóp landsmanna, enda er vernd íslenskra fjarskiptaneta eitt af markmiðum sveitarinnar.

Markmiðið hér er að veita sérfræðiráðgjöf um einstök málefni og ef svo ber undir að gefa leiðbeiningar þessu tengt. Áhersla er á ómissandi upplýsingainnviði en ráðgjöf og leiðbeiningar geta líka náð til annarra innviða, sem og fólks almennt, ef og þegar töluverð hætta er á ferðum.

4. Almenn upplýsingaöflun

Sveitin fylgist með ógnum og öryggisatvikum með ýmsu móti, m.a. með upplýsingasöfnun í gegnum samstarfssamninga við ýmsa innlenda og erlenda aðila. Einnig er fylgst með þróun mála hjá sysurhópum og öðrum traustum aðilum um nýja veikleika og aðferðir í netárásum. Með þessu hefur sveitin sýn yfir aðsteðjandi ógnir.

Mikilvægt er að heildaryfirsýn sé yfir hvað er að gerast þegar kemur að ógnum og öryggisatburðum með það að markmiði að forðast ógnir, bregðast fyrr við og með markvissum hætti, og veita ráðgjöf og leiðbeiningar eftir þörf.

5. Almenn vitundarvakning

Sveitin heldur úti opna vefsetrinu www.cert.is. *Jafnframt heldur Póst- og fjarskiptastofnun úti vefsetrinu* www.netöryggi.is *með almennum upplýsingum um netöryggismál fyrir almenning og smærri fyrirtæki.*

Markmiðið hér er að allir hérlendis geti fengið upplýsingar um almennar varnir, góð varnarráð og svo framvegis í gegnum vefsetur í umsjón sveitarinnar. Ekki er um það að ræða að svara einstökum fyrirspurnum sem kunna að berast, svo sem frá einstaklingum, en það fer þó eftir mikilvægi mála og hvaða innviðir gætu verið í hættu.

6. Regluleg skýrsla

Árlega birtir netöryggissveitin skýrslu þar sem m.a. er fjallað um ógnir og öryggisatvik hérlendis og almennan fróðleik um netöryggismál.

Markmiðið með þessu er að gera starfsemi sveitarinnar gegnsærri með útgáfu ársskýrslu, þar sem farið er yfir síðasta starfsár, stöðuna um áramót, ógnir ræddar, framtíðarmöguleikum velt upp o.s.frv.

7. Alþjóðlegt samstarf

Sem landstengiliður fyrir Ísland tekur sveitin þátt í alþjóðlegu samstarfi og átaksverkefnum um CERT-málefni og öryggi ómissandi upplýsingainnviða (ÓUI). Enn fremur er hún þátttakandi í norrænu samstarfi CERT-netöryggissveita um gagnkvæm upplýsingaskipti, þar sem skipst er á margs konar gögnum um öryggisatvik, varnir og viðbúnað.

Markmiðið hér er að efla erlent samstarf sveitarinnar við sambærilega aðila erlendis, svo sem aðrar netöryggissveitir og alþjóðlegar stofnanir. Þar ber fyrst að nefna samstarf við sambærilegar sveitir á Norðurlöndunum, síðan almennt samstarf innan Evrópu í gegnum ENISA – stofnun ESB um netöryggismál, og að lokum samstarf við aðra aðila. Er þetta einn stærsti þátturinn í CERT starfi almennt, þar sem öryggisatvik snerta yfirleitt fleira en eitt land.

Eins glímum við við svipaðar ógnir og nágrannaþjóðir okkar, en samvinna þeirra hefur eflt þær í störfum sínum og skilað betri skilningi á því sem er í gangi hverju sinni.

Stærri atvik sem sveitin fékkst við á árinu 2013

BGP vandamál hjá Símanum (meintur umferðarstuldur)

Í ágúst 2013 kom upp óþekkt bilun í einum netbeini Símans í borginni Toronto í Kanada sem olli því að send voru út röng BGP umferðarstjórnunarmerki (e. Border Gateway Protocol) til mótaðila í IP flutningsleiðum. Merkin gáfu til kynna að nokkrir viðskiptavinir Símans, sem hafa eigin AS númer væru móttökuaðilar fyrir tilteknar blokkir af IP tölum, sem eru í raun notuð annars staðar í heiminum. Afleiðingar þessa voru að hluti umferðar sem átti endastöð í þeim IP tölum var beint um net Símans á Íslandi áður en henni var komið til réttra aðila. Þar sem kerfi Símans bjó yfir réttum upplýsingum var umferðinni komið á réttan endapunkt með örlítilli töf.

Frétt um málið var birt af erlendu fyrirtæki í nóvember þar sem þessi bilun var tengd öðru svipuðu máli og leiddar að því líkur að um viljaverk einhvers aðila væri að ræða. Var ýjað að því að íslensk fyrirtæki stæðu fyrir gagnastuldi og var umfjöllunin frekar neikvæð, sérstaklega þá fyrir Símann. Í kjölfarið var farið nákvæmlega yfir málið bæði hjá Símanum og netöryggissveitinni. Í ljós kom að um galla í hugbúnaði beinisins sem Síminn var að nota var að ræða. Staðfesting á því fékkst að lokum frá framleiðanda búnaðarins og birti hann skýrslu um gallann á þjónustuvef sínum.

Vodafone málið

Laust eftir miðnætti þann 30. nóvember, 2013 voru vefsíður Vodafone á Íslandi eyðilagðar, meðal annars þjónustusíður fyrirtækisins, og markaði það enda innbrots á vefþjóna fyrirtækisins. Stuttu síðar var miklu af viðkvæmum gögnum lekið á netið sem stolið hafði verið í því innbroti.

Þau vefkerfi Vodafone sem um ræðir samanstanda af ytri vefþjóni og tengdum gagnagrunni. Aðdragandi innbrotsins virðist hafa verið með þeim hætti að ytri vefþjónninn var skannaður með ýmsum aðferðum, í þeim tilgangi að finna veikleika sem síðan væri hægt að nota til að brjótast inn á vefþjóninn. Slíkur veikleiki fannst og það gerði tölvuþrjótinum kleift að hlaða upp „bakdyrum “ inn á vefþjóninn það sama kvöld. Þetta veitti honum nánast fullkominn aðgang að þjóninum. Veikleikinn sem um ræðir var svokallaður „upload-execute“ veikleiki og kom til vegna forritunarvillu í sérsniðnu vefkerfi Vodafone.

Afleiðingar þessa aðgangs var sá að tölvuþrjóturinn gat náð í afrit af gögnum úr gagnagrunni tengdum vefkerfinu og síðan reynt að eyða slóð sinni og eyðileggja vefsíður Vodafone aðfaranótt 30. nóvember. Nokkrum klukkustundum síðar var gögnum sem stolið var frá Vodafone dreift á hinu almenna interneti og auglýsing um það birt á Twitter.

Í atvikinu reyndi í fyrsta sinn á skipulag, þekkingu og reynslu netöryggissveitarinnar við að meðhöndla stór öryggisatvik undir tímapressu. Strax og sveitin var orðin meðvituð um atvikið voru viðeigandi verkferlar virkjaðir og unnið eftir þeim í gegnum allt atvikið. Á heildina litið

virkuðu verkferlar netöryggissveitarinnar að mestu í samræmi við fyrirætlanir. Fjölmörg atriði komu þó í ljós sem lagfæra þarf í starfi sveitarinnar, lagaumhverfinu og í samskiptum við ytri aðila.

Þegar starfsmenn CERT-ÍS voru kallaðir út var nokkuð liðið frá því að innbrotið uppgötvaðist, eða um 11 klukkustundir. Nauðsynlegt er að gera viðeigandi breytingar á fyrirkomulagi tilkynninga til sveitarinnar, sem og á starfstíma hennar, svo stytta megi þennan tíma verulega.

Þegar atvikið er rýnt er ljóst að bæta þarf öflun og miðlun upplýsinga um yfirstandandi atvik þar sem miðlun slíkra upplýsinga innan þjónustuhópsins er ein helsta og áhrifamesta aðgerðin sem sveitin hefur á sínu valdi. Án slíkra upplýsinga eru aðrir aðilar í mikilli óvissu um öryggi eigin kerfa og verða því óhjákvæmilega að fara í mögulega óþarfan viðbúnað.

Atvik þetta og afleiðingar þess eru alvarlegar fyrir þá sem hafa orðið fyrir tjóni af völdum þess, beint eða óbeint. Þar sem þetta atvik beindist fyrst og fremst að einum aðila reyndi ekki mikið á samhæfingarhlutverk netöryggissveitarinnar í þessu tilviki. Hins vegar sinnti hún ýmsum öðrum þáttum s.s. greiningu, upplýsingamiðlun o.fl. Þetta atvik sýndi ljóslega að geta sveitarinnar til að sinna útbreiddari atvikum er takmörkuð af núverandi stærð hennar.

Fjallað er nánar um atvikið í sérstakri skýrslu CERT-ÍS sem finna má á heimasíðu sveitarinnar.

Erlent samstarf

Netið byggist á því að tengja saman fólk og tæki um heim allan. Þegar kemur að netöryggi skiptir samstarf milli þjóða því gríðarlega miklu máli, þar sem ógnir eru í fæstum tilfellum bundnar við eitt land eða afmarkað svæði. Einnig verður að gera ráð fyrir ógnum sem eru það umfangsmiklar að þær geta ógnað verulega öryggi fleiri þjóða samtímis.

Alþjóðlegt samstarf er jafnframt mikilvægt til að deila reynslu og lærdómi í þeim tilgangi að samræma og gera viðbúnað og viðbrögð sem skilvirkust.

Norrænt samstarf

Norrænt samstarf í netöryggismálum er mjög ofarlega í forgangi hérlendis og grundvallast á samkomulagi milli Norðurlandaþjóðanna á sviði CERT-málefna. Í undirbúningi er uppsetning á sameiginlegu norrænu upplýsingaskiptaneti sem netöryggissveitin CERT-ÍS á hlut að sem landstengiliður fyrir Ísland. Upplýsingaskiptanetið er nauðsynlegt tól fyrir gagnkvæm upplýsingaskipti, þar sem skipst er á margs konar gögnum um öryggisatvik, varnir og viðbúnað.

Reynsla af þessu er mjög góð og lagt er til að norrænt samstarf á þessu sviði verði eflt enn frekar á komandi árum, svo sem með þátttöku í sameiginlegum æfingum Norðurlandanna, með auknum upplýsingaskiptum, starfsmannaskiptum o.fl.

Samstarf við ENISA

Póst- og fjarskiptastofnun hefur um árabil átt í góðu samstarfi við Net- og upplýsingaöryggisstofnun Evrópusambandsins, ENISA, ekki síst um CERT málefni og málefni ómissandi upplýsingainnviða, um stefnu ESB í netöryggismálum o.s.frv. Er þessi samvinna eitt af forgangsverkefnum CERT-ÍS, enda nýtist þaðan mikil reynsla og þekking á þessu sviði.

Vaxandi ógnir og önnur mál

Árið 2013 var margt í gangi sem snerti alþjóðleg netöryggismál. Mikil umfjöllun hefur verið erlendis um gagnaleka og möguleika til njósna og hlerana. Oft eru markmið með netárásum þó að auðgast, eyðileggja og upphefja sjálfan sig. En hverjar sem hvatirnar eru þróast tækni og aðferðir til að fremja netglæpi í takt við aðra tækni og því þurfa netöryggisaðilar stöðugt að uppfæra þekkingu sína og vera á varðbergi gagnvart nýjungum.

Ein meginleið sem notuð er við tæknilegar netárásir er misnotkun veikleika, og í desember 2013 fannst veikleiki í NTPd hugbúnaðinum. Sá hugbúnaður sér um að samstilla klukkur í tölvum tengdum netinu. Þennan veikleika má hins vegar nýta til að valda þjónusturofi (e. Denial of Service attack) með umferðarmögnun (e. amplification attack) á þriðja aðila. Þannig er það ekki endilega fórnarlambið hverju sinni sem er með veikan NTPd þjón. Á svipaðan hátt er hægt að nota nafnaþjóna (DNS) til árása, séu þeir rangt stilltir.

Svokölluð dulrán (e. Ransom-ware) , eitt form fjárkúgana, fer vaxandi og þekkjast dæmi þess hérlendis. Um er að ræða óværu sem dulritar öll gögn á tölvu fórnarlambsins, komist hún þar inn. Þegar því er lokið er upprunalegu gögnunum eytt og viðkomandi er boðið að kaupa lykilinn til að komast aftur í gögnin sín. Því vill netöryggissveitin hvetja almenning og fyrirtæki til að eiga góð og örugg afrit af öllum gögnum sem viðkomandi telur mikilvæg, hvort sem um er að ræða fjölskyldumyndir, lokaritgerðir, eða viðskiptamannaskrár fyrirtækja. Slík afrit skal geyma ótengd tölvunni.

Mikil aukning í afkastagetu farsíma, bæði í afli og tengigetu með nýrri kynslóð fjarskiptaneta, ýtir undir vaxandi þróun ógna á þessu sviði tækninnar. Óværur eru ekki óþekktar í þessum hluta netsins ásamt öðrum vandamálum svo sem svindlskilaboðum með SMS.

SCADA kerfi eru notuð til að stjórna ýmsum búnaði í iðnaði, við raforkuframleiðslu o.s.frv. Meðal annars stýra slík kerfi flutnings- og dreifikerfum raforku. Hvers konar hættur sem steðja að þeim kerfum stofna því um leið raforkuflutningum í hættu. Í slíkum tilfellum verða SCADA kerfin að teljast hluti af ómissandi upplýsingainnviðum landsins. Annars staðar eru þau það ekki, svo sem SCADA kerfi sem stýra minni kerfum, t.d. í einstökum byggingum/fyrirtækjum.

Hér á landi sem annars staðar er mikil umræða um kosti þess og galla að geyma gögn í netskýjum. Einn þeirra galla sem bent hefur verið á er sá að yfirleitt eru þessi netský erlendis og undir eftirliti þar til bærra yfirvalda í hverju landi fyrir sig. Slíkt getur valdið ýmsum vandkvæðum og almennt mælir netöryggissveitin með því að stjórnvöld, fyrirtæki og einstaklingar hafi varann á sér og meti hvort hýsa eigi viðkvæm gögn hérlendis.

Starfsáætlun fyrir 2014 og áherslur

Áherslur á nýju ári verða meðal annars:

- ✓ Vefgátt og upplýsingaskiptakerfi við þjónustuhópinn þróuð áfram þar sem lögð verður áhersla á samhent viðbrögð þjónustuhópsins í stærri málum, að aðilar geti sent viðvaranir beint á aðra aðila, hægt verði að senda tilkynningar til sveitarinnar o.s.frv.
- ✓ Enn meiri áhersla á sameiginlegar æfingar, svo sem sameiginlega æfingu netöryggissveita Norðurlandanna, CE-2014.
- ✓ Sérstökum samráðsvettvangi komið á um stærri mál sem kunna að koma upp
- ✓ Endurbætur í kjölfar Vodafone málsins
- ✓ Útvíkkun þjónustuhóps sveitarinnar
- ✓ Efla og prófa reglulega gæði sveitarinnar er lýtur að innri málum, svo sem verkefnum og verkferlum, þjálfun starfsmanna o.s.frv.