Efnisyfirlit

Frá hópstjóra sveitarinnar

Skýrsla sú sem hér birtist er önnur ársskýrslan sem netöryggissveitin CERT-ÍS sendir frá sér. Henni er ætlað að veita innsýn í starfsemi og viðfangsefni sveitarinnar á árinu 2014.

Hugtakið netöryggissveit er þýðing á hinu enska heiti Computer Emergency Response Team (skammstafað CERT) og þjónar sveitin fyrst og fremst fjarskiptamarkaðnum. Hún hefur þó heimild til að gera samninga við aðra aðila í öðrum geirum sem teljast til ómissandi upplýsingainnviða og var unnið markvisst að því á fyrri hluta ársins þar sem fókusinn var tekinn á orkugeirann til að byrja með. Vanda þarf til verka þegar slíkt skref er stigið, svo sem að starfsmenn þekki til viðkomandi geira og að til staðar sé nægur mannskapur til að sinna þeim verkefnum sem upp kunna að koma. Ekki tókst sem skyldi að klára samningana og urðu til þess ýmsar orsakir. M.a. varð sú stefnubreyting á vormánuðum hjá þáverandi innanríkisráðherra að flytja ætti starfsemi sveitarinnar til almannavarnadeildar ríkislögreglustjóra og ætti flutningurinn að ganga hratt og greiðlega fyrir sig. Þar sem tilvist sveitarinnar og starfsemi hennar eru skilgreind í fjarskiptalögum og sérstakri reglugerð, þá þurfti lagabreytingu til, sem og breytingu á reglugerð ráðuneytisins um starfsemi hennar og verkefni. Stækkun þjónustuhópsins var því ekki lengur á dagskrá, þar sem ekki var ljóst hvaða stefna yrði tekin í samstarfi sveitarinnar við aðra geira en fjarskiptamarkaðinn og eins hvort um slíkt samstarf yrði að ræða yfirhöfuð. Þáverandi fjárheimildir PFS náðu ekki að standa undir rekstri sveitarinnar nema samningar yrðu gerðir við hóp aðila úr hverjum geira fyrir sig. Ýmislegt varð því til að tefja stækkun þjónustuhópsins. Við þetta bættist að hvorki tókst að koma frumvarpi um þetta mál í gegn á vorþinginu 2014, né á haustþinginu. Þetta gerði það að verkum að ýmis verkefni sveitarinnar voru upp frá þessu í óvissu og hreinlega náðust ekki fram, svo sem tenging við samnorrænt upplýsingaskiptanet (Nordic CERT Information Sharing Network). Þar að auki var fjármögnun ekki í þeim föstu skorðum sem starfsmenn og stjórnendur PFS höfðu gert sér vonir um. Meiri óvissa og minni bjartsýni um framhaldið voru því ríkjandi en árið áður. Tveir starfsmenn sveitarinnar létu af störfum og kom einn í staðinn. Við árslok var því heildarfjöldi starfsmanna tveir, í stað þriggja. Það má telja of lítið fyrir starfsemi sem þessa ef vel á að vera.

Upp frá þessu þróuðust málin þannig að sveitin varð að einbeita sér að eigin kjarnahóp, sem eru stærri fjarskiptafyrirtæki en láta aðra geira um að bjargast að mestu leyti á eigin spýtur. Sem netöryggissveit á landsvísu, er það þó almennt markmið sveitarinnar að aðstoða þá aðila eins og efni eru til. Slík mál hafa þó aldrei forgang yfir önnur verkefni sveitarinnar sem eru ærin. Þessi þróun var óumflýjanleg eftir það sem á undan var gengið. Um áramótin 2014/1015 var staðan því sú að hvorki var mögulegt að taka banka- né orkugeirinn inn í í þjónustuhóp sveitarinnar. Þegar þetta varð ljóst var vefsíða sveitarinnar endurgerð og textinn einfaldaður til að endurspegla einfaldari og breytta starfsemi frá því sem upphaflega var stefnt að, þ.e. að sveitin ynni með ómissandi geirum þjóðfélagsins.

Undir lok ársins 2014 , voru ekki fyrirséðar frekar breytingar á starfsemi sveitarinnar eða fjármögnun. Hvorki varðandi það sem sneri að breyttum lagaramma um starfsemina né að meiri samvinnu með öðrum geirum og eflingu á norrænu og öðru erlendu samstarfi og upplýsingaskiptum. Helgast þetta af því að málefni um framtíð sveitarinnar hafa ekki verið tekin fyrir á Alþingi.

Sveitin fæst að öllu jöfnu við töluverðan fjölda mála vegna netöryggisatvika sem má segja að séu í venjulegum forgangi sveitarinnar. Hins vegar koma stundum upp mál sem eru alvarlegri og fékkst

sveitin við a.m.k. þrjú slík mál á árinu. Þetta voru m.a. netárás gegn þjónustu, sem veitt er af einu af stærri fjarskiptafyrirtækjunum, til að trufla útlandasamband þess. Ennfremur fór töluverður tími í að samræma aðgerðir hérlendis gagnvart óværum sem hafði verið plantað í hýsta netþjóna til að nota til ýmissa glæpaverka, eða tölvur sem hafa verið teknar yfir af svonefndum botnetum eða laumunetum af ýmsum ástæðum. Má segja að málum sem þessum fari fjölgandi. Sveitin fékk ennfremur þó nokkuð af fyrirspurnum erlendis frá, sem snérust um skannanir á veikleikum netsins af íslenskum aðilum. Kviknuðu spurningar um lögmæti slíkra skannanna.

Alvarlegustu málin eru þau sem má flokka sem APT (Advanced Persistence Threat) en það eru mjög alvarlegar ógnir sem ógna öryggi ríkisins, stuldur á iðnaðarleyndarmálum og fleira í þeim dúr. Bak við þær standa aðilar sem gefa sé góðan tíma til að ná fyrirfram vel skilgreindu marki sínu, svo sem að ná í afar viðkvæmar upplýsingar úr upplýsingatæknikerfum. Erlendis frá eru dæmi um að slíkar ógnir komi upp í ráðuneytum landa. Þessar ógnir er mjög mikilvægt að hindra með bestu öryggisráðstöfunum og leita uppi með viðeigandi skynjarabúnaði.

Vegna fyrrgreindrar óvissu um stöðu og starfsemi sveitarinnar, var farið hægar í ýmsar áætlanir, svo sem að koma á samhæfingar- og samræmingarhlutverki innan netumdæmisins með markvissum upplýsingaskiptum og neyðarsamráði.

Netöryggissveitin CERT-ÍS tók þátt í fyrsta hluta af þremur í sam-evrópskri netöryggisæfingu (CE-2014) á vegum ENISA, sem er sú stofnun ESB sem sinnir netöryggismálum og vernd mikilvægra innviða álfunnar. Vegna þeirra þrenginga sem sveitin og starfsemin gekk í gegnum var ekki talið stætt á öðru en að láta eingöngu fyrsta hluta æfingarinnar duga og sitja hjá í öðrum og þriðja hluta æfingarinnar.

Verst er þó að geta ekki verið samstíga hinum Norðurlöndunum í uppbyggingu hins fyrrgreinda gagnkvæma upplýsingaskiptanets. Þetta upplýsinganet nýtist vel þegar Norðurlöndin þurfa að veita viðkvæmar upplýsingar tengdar netöryggismálum, sem og að veita hvert öðru aðstoð og stuðning.

Árið 2014 var, eins og 2013, viðburðarríkt þegar litið er til netöryggismála. Sveitin vann að tveimur málum sem flokkast sem alvarleg og gaf út tvær almennar viðvaranir. Sem fyrr kom einnig töluverður fjöldi minni mála til meðferðar hjá netöryggissveitinni á árinu. Ekki verður nánar gerð grein fyrir þeim hér, en þau koma fram í tölfræði um starfsemina. Ennfremur skrifaði sveitin skýrslu um netárás á Vodafone frá árinu áður og má ennfremur finna hana á heimasíðu sveitarinnar.

Ógnir virðast aukast milli ára og er fyrirséð að sú þróun haldi áfram á næstu árum. Í kjölfar væntanlegs lagafrumvarps er því æskilegt að stækka þjónustuhóp sveitarinnar þannig að starfsemi hennar nái einnig til fyrirtækja og stofnana utan fjarskiptamarkaðarins, svo sem í orku- og fjármálageiranum sem eru lykilgeirar þjóðfélagsins

Á verkefnasviðinu verður miðað við óbreytt ástand í takt við ríkjandi lagaumhverfi og samninga sveitarinnar. Lögð verður áhersla á að þjónusta fjarskiptamarkaðinn nær eingöngu. Þó væri æskilegt að geta unnið að uppbyggingu á ástandsvitundarsetri 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 væri mjög mikilvægt að CERT-ÍS yrði gert kleift að tengjast sameiginlegu upplýsingaskiptaneti norrænna netöryggissveita, en þetta er eitt af því sem nú er brýnast svo sveitin geti sinnt verkefnum sínum.

Segja má að sveitinni hafa ekki tekist nægjanlega að styðja við að öryggisatvik séu tekin föstum tökum af þjónustuhópi sveitarinnar. Helgast það að stórum hluta til af því millibilsástandi sem sveitin var í stóran hluta ársins 2014 en bein afleiðing þess var að starfsmenn sveitarinnar voru aðeins tveir seinni hluta ársins. Á fyrri hluta ársins 2015 eru framtíðarhorfur sveitarinnar mun dekkri en á sama tíma árið á undan. Það er þó er von starfsmanna CERT-ÍS að tekið verði föstum tökum á málefnum sveitarinnar og framtíðarstöðu hennar bæði í þinginu og í innanríkisráðuneytinu sem allra fyrst.

Stefán Snorri Stefánsson

Hópstjóri CERT-ÍS netöryggissveitarinnar

Yfirlit 2014

Á fyrsta heila starfsári sveitarinnar var unnið að ýmsum málum fyrir utan daglegan rekstur. Uppbyggingu kerfis til að miðla sjálfvirkt upplýsingum um öryggisatvik var lokið að mestu hvað varðar að sveitin geti sent frá sér upplýsingar, vefsíða sveitarinnar var endurbætt, verklagsreglur endurgerðar og fleira gert er snýr að slíkri starfsemi.

Daglegur rekstur

Öryggisatvik sem teljast til þeirra sem kalla má að hafi venjulegan forgang eru daglegt brauð í rekstri netöryggissveita. Flest þessara atvika þarf sveitin ekki að fara djúpt ofan í, heldur miðla upplýsingum um þau til hlutaðeigandi aðila og fylgjast með framþróun þeirra. Það sem var áberandi og vaxandi á árinu voru svokölluð Phishing blekkingarmál og netárásir gerðar til að skerða þjónustu fyrirtækja. Dæmi um þetta voru tímabundnar Phishing árásir á fjarskiptafyrirtæki og banka hérlendis og markviss netatlaga gegn útlandasamböndum eins fjarskiptafyrirtækis. Samvinna við hagsmunaaðila reyndist vel, t.d. viðeigandi lokanir til að hindra frekara tjón.

Oft verður sveitin áskynja um, eða hefur vitneskju um, mál sem telja má það alvarleg að gefa þurfi út almenna viðvörun vegna þeirra á vefsíðu sveitarinnar. Dæmi um slíkt eru svokölluð Hearthbleed/Poodle og Bash (Shellshock) mál. Ennfremur færðust í vöxt svokölluð Cryptolocker mál.

Á árinu kom töluverður fjöldi atvika til kasta sveitarinnar varðandi tölvur sem hafa flækst í net botneta og eru notaðar til margs konar glæpsamlegra aðgerða.

Önnur atvik voru meðhöndluð eftir viðeigandi ferlum en ekki rata öll þeirra í opinbera umræðu af ýmsum ástæðum. Er stiklað á stóru um þau hér á eftir í tölfræðiupplýsingum.

Kerfi til upplýsingamiðlunar

Ein meginstoðin í starfsemi netöryggissveitarinnar er miðlun upplýsinga um öryggisatvik, hættur og annað. Er tilvist slíks kerfis og frekari þróun mikill styrkur fyrir netöryggissveitina, þar sem sjálfvirkni og sjálfsafgreiðsla eru mikilvægir þættir. Jafnframt var á árinu opnaður þjónustuvefur fyrir þá aðila sem sveitin sinnir, með það að markmiði að samþætta hann við sjálfvirka upplýsingamiðlunarkerfið.

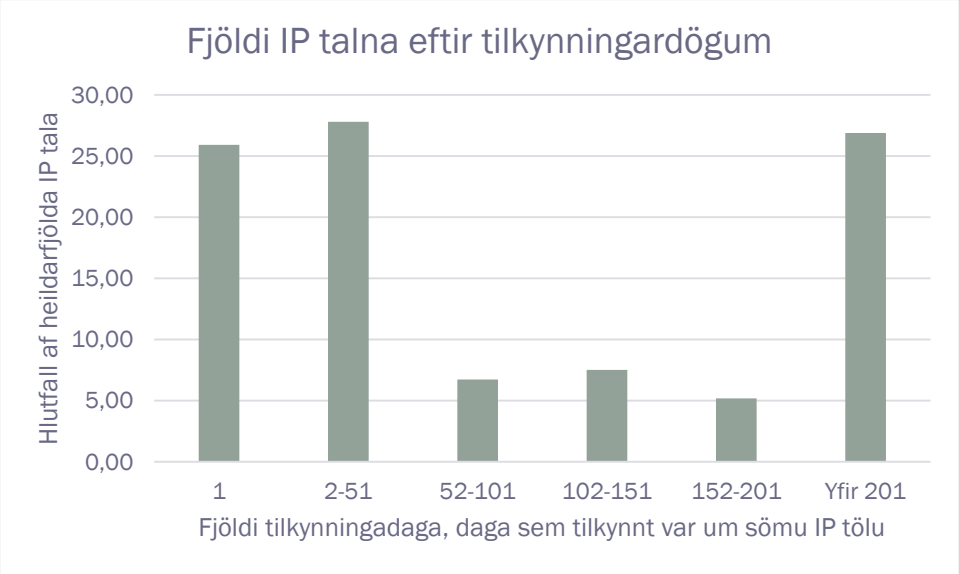
Lykiltölur um upplýsingamiðlun

CERT-ÍS fylgist á hverjum tíma með stöðu netöryggisatvika, stórra sem smárra, sem eru innan netumdæmis sveitarinnar. Að auki fær sveitin líka upplýsingar um atvik utan umdæmisins, en þau eru öllu færri þar sem langstærstur hluta IP talna á Íslandi fer í gegnum fjarskiptafyrirtækin . Tekið skal fram að í þessari samantekt eru atvik í fjarskiptanetum RHnets ekki með, enda heyra þau undir umdæmi net- og háskólasamfélagsins.

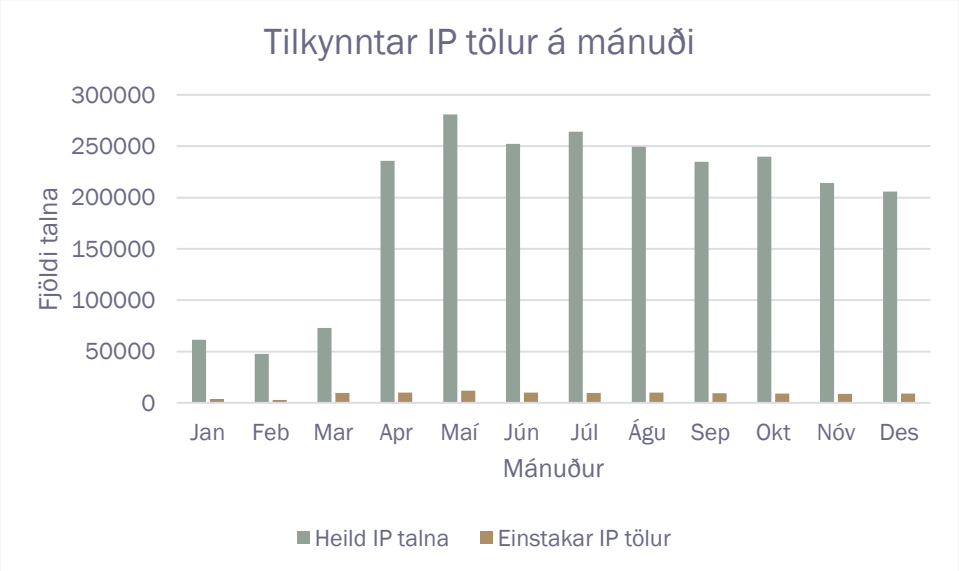
Árið 2014 var tilkynnt um 21656 IP tölur sem netinu hérlendis stafaði ógn af á mismunandi hátt. Af þeim voru 5609 IP tölur þar sem tilkynningar stóðu aðeins yfir í einn dag eða skemur. Fjöldi IP talna þar sem tilkynningar um sömu IP töluna stóðu lengur yfir, voru of margar að okkar mati. Af þessu má greina að betur þarf að standa að því að leysa vandamál sem upp

koma og bregðast fyrr við. Þetta þýðir að sveitinni hefur ekki tekist það ætlunarverk sitt að fá samstarfsaðila/notendahópinn til að bregðast við, eða upplýsa nægjanlega um hvað er á ferðinni hverjum tíma (Sjá Mynd 1).

Mynd 1.



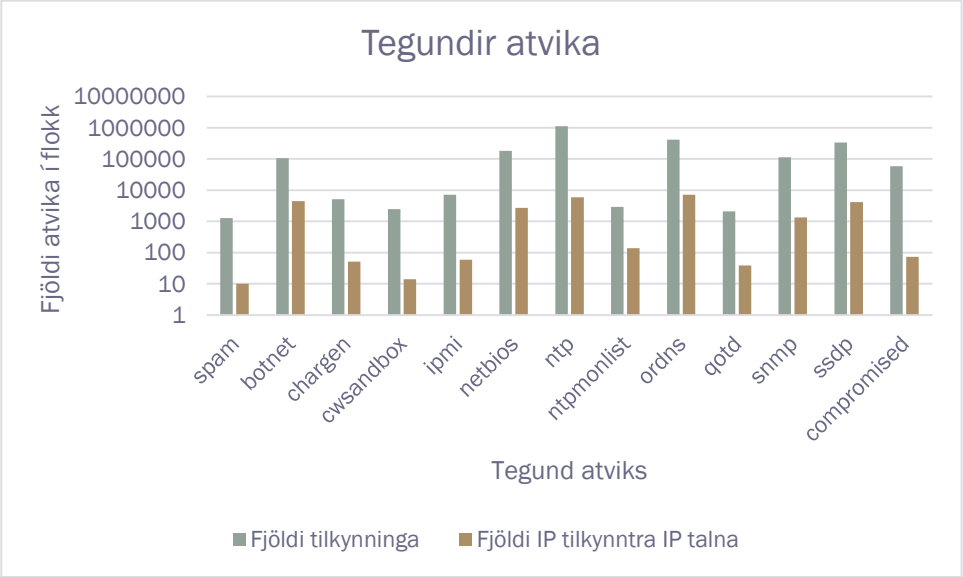
Mynd 2.



Á mynd 2 sýna hærri súlurnar hversu margar tilkynningar berast sveitinni. Hins vegar lýsa lægri súlurnar einstökum IP tölum sem tengjast atvikum og eru þær nokkuð vaxandi fram eftir árinu. Þess má geta að í apríl kemur fram svokallaður Heartbleed veikleiki í OpenSSL og í september veikleiki í Bash sem heitir ShellShock.

Minni atvik sem tilkynnt er um eru mjög mismunandi, en skiptingu þeirra í helstu flokka yfir árið má sjá á mynd 3. Athygli vekur að mikið hefur borist af tilkynningum um NTP (Network Time Protocol).

Mynd 3.



Á mynd 3 standa gráu súlurnar fyrir fjölda tilkynninga fyrir sérhvern flokk öryggisatvika. Aftur á móti tákna brúnu súlurnar fjölda IP talna sem tilkynnt var um fyrir hverja þessara ógna.

Stefnumótunarvinna

Eins og nefnt var í síðust ársskýrslu er hópstjóri hennar áfram þátttakandi í vinnuhóp innanríkisráðuneytisins í verkefninu um mótun á netöryggisstefnu Íslands. 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

Í boði almannavarna Svíþjóðar (MSB), sóttu meðlimir netöryggissveitarinnar undir lok ársins SCADA (Supervisory Control And Data Acquisition) netöryggistengt iðnaðarstýringarnámskeið í Linköping í Svíþjóð. Reynslan af námskeiðinu var mjög góð, og ekki síður þau tengsl sem mynduðust við Norðurlandaþjóðirnar á þessu sviði. Þekkingin sem þarna fékkst nýtist til að vinna með og byggja upp þekkingu á netöryggi iðnaðarstýringarkerfa sem m.a. eru notuð hérlendis í raforkuiðnaði. Eru starfsmenn sveitarinnar nú betur í stakk búnir til að koma að netöryggi slíkra kerfa.

Æfingar hafa til þessa reynst vel til þess að samræma viðbrögð og ferla og efla tengsl aðila á markaði. Mikilvægt er að sem flestir þjónustuaðilar taki þátt í slíkum æfingum í að verjast þeim netógnum sem steðja að í netheimum nútímans, hvort sem um er að ræða minni eða stærri ógnir.

Netútlaginn

Árið 2013 var síðast haldin innanlands æfing þjónustuhóps sveitarinnar í netöryggismálum. Stefnt er að því að halda slíka æfingu annað hvort ár og því verði Netútlaginn aftur haldinn á árinu 2015. Alls ekki er víst að það markmið náist, þar sem fyrirséð umrót í tengslum við hugsanlegan flutning sveitarinnar gæti kippt grundvellinum undan slíkri æfingu. Þrátt fyrir

það huguðu sveitarmeðlimir á árinu 2014 að fyrirkomulagi næsta Netútlaga, sviðsettum atburðum og öðrum þáttum undirbúnings.

Samevrópsk netvarnaræfing, Cyber Europe 2014

Á árinu var haldin samevrópsk netvarnaræfing ESB/ESS þjóða, með þátttöku netöryggissveita, einkaaðila og opinberra stofnana. Æfingin er haldin annað hvort ár. Henni var núna skipt í þrennt; tæknilegan hluta, samvinnuhluta og í þriðja hluta var unnið með ákvarðanir á stefnumótunarstigi. CERT-ÍS tók þátt í fyrsta hlutanum með stærstu aðilum úr orkugeiranum. Voru menn á einu máli um að vel hefði tekist til. Því miður sáu aðilar fjármálamarkaðarins sér ekki fært að vera með. Það, ásamt því hversu erfitt reyndist að fjármagna frekari þátttöku sveitarinnar í CE-2014 varð þess valdandi að alfarið var hætt við að taka þátt í hluta tvö og þrjú. Aftur á móti er stefnt að því að taka fullan þátt í undirbúningi og framkvæmd CE-2016 ef aðstæður leyfa.

Starfsemi sveitarinnar

Til áréttingar er rétt að nefna að starfsemi og þjónusta CERT netöryggissveita snýst ekki um bein inngrip í netkerfi og þjónustu þeirra aðila sem sveitin þjónar, heldur er um að ræða tilmæli og ráðgjöf varðandi viðbrögð, bæði varðandi fyrirbyggjandi skipulag og aðgerðir og hvað beri að gera þegar öryggisatvik koma upp.

Þjónusta sveitarinnar tekur mið af ákvæðum laga og reglugerðar um starfsemi sveitarinnar.

Þjónusta CERT-ÍS skiptist í höfuðdráttum í tvennt; svokallaða kjarnaþjónustu og þjónustu á landsvísu.

Kjarnaþjónusta sveitarinnar snýr fyrst og fremst að fjarskiptafyrirtækjum sem mynda þjónustuhóp hennar. Auk kjarnaþjónustunnar veitir sveitin vissa þjónustu fyrir allt landið, svokallaða landsþjónustu.

Hér á eftir er hverri þjónustu lýst í grófum dráttum eins og henni var breytt undir lok ársins 2014. Lýsingin getur sem fyrr tekið breytingum á hverjum tíma í takt við tæknibreytingar og fleira. Í starfsemi sveitarinnar og innan þjónustuhóps hennar er lögð áhersla á góð upplýsingaskipti um öryggisatvik og fleira tengt netöryggismálum.

Gildandi lýsingu á þjónustu sveitarinnar á hverjum tíma má finna á vefsíðu hennar (www.cert.is).

Þjónusta CERT-ÍS

Sem fyrr segir var þjónustan einfölduð töluvert undir lok ársins 2014, m.t.t. þeirrar staðreyndar sem ljós varð í lok árs að sveitin væri ekki á förum til almannavarnadeildar RLS eins og innanríkisráðherra hafði áætlað á fyrri hluta ársins. Einnig hafði þrengt töluvert að sveitinni varðandi fjármagn til starfseminnar og starfsmönnum hennar til að sinna starfseminni hafði fækkað. Hér er þjónustunni lýst í þessari breyttu mynd.

Kjarnaþjónusta

Hér á eftir er upptalning á kjarnaþjónustu CERT-ÍS sem er fyrir þjónustuhópinn einvörðungu og tæknilega innviði hans, svokallað netumdæmi sveitarinnar. Landsþjónusta er annað og er lýst hér aftar.

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

1. Meðferð vegna öryggisatvika í venjulegum forgangi

Meðhöndlun öryggisatvika er visst vinnuferli í kringum úrlausn öryggisatvika sem hafa venjulegan forgang í vinnslu sveitarinnar. Sveitin gerir forgreiningu og í kjölfarið leggur af stað með/ ráðleggur og/eða aðstoðar við að hrinda ákveðnum viðbrögðum af stað innan netumdæmisins. Sveitin samræmir aðgerðir sé þess þörf og gerir öðrum viðvart, ef svo ber undir.

2. Meðhöndlun alvarlegri öryggisatvika/stóráfalla

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

Til að auðvelda þetta er fyrirfram myndaður samráðsvettvangur sem getur ýmist verið um tiltekin málefni eða innan þess geira þjóðfélagsins sem viðkomandi aðili er í.

Í samvinnu við þjónustuhópinn vinnur sveitin að því að efla sem best ástandsskilning (Situation Awareness) í neyðarástandi. Þetta snýst m.a. um að sveitin útbýr yfirlit yfir ástandið, gerir tæknilega lýsingu á vandamálinu, hvaða áhrif það hefur/getur haft, hvaða verkfæri, aðstaða og mannafli eru til reiðu og hvaða aðgerðir eru í gangi. Einnig er metið hvaða næstu skref þykja æskileg. Tilgangurinn er að stuðla að réttri ákvarðanatöku þegar á reynir, sem og að virkja nauðsynlegar viðbragðsáætlanir tímanlega.

Til að efla neyðarviðbrögð og -varnir enn frekar fyrirfram, stendur sveitin fyrir og/eða tekur þátt í netöryggisæfingum (Cyber Exercises) sem fyrst og fremst snúa að þjónustuhópnum. Í æfingunum eru yfirleitt sviðsett alvarleg öryggisatvik/stóráföll svo ímyndað neyðarástand skapist. Áhersla í æfingum er breytileg, sem og hverjir innan þjónustuhópsins taka þátt hverju sinni. Æfingar geta verið alþjóðlegar eða bundnar við Ísland.

Landsþjónusta

Landsþjónusta netöryggissveitarinnar er ekki hluti af kjarnaþjónustu hópsins, heldur styður hún við öryggismál í netumdæminu sem kjarnaþjónustan snýr að, jafnframt því að efla almennt netöryggi innanlands.

1. Landstengiliður

CERT-ÍS er landstengiliður (e. National Point of Contact) um CERT-málefni og öryggi ómissandi upplýsingainnviða (ÓUI). Þetta innifelur m.a. 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.

Sveitin tekur þátt í alþjóðlegu samstarfi og átaksverkefnum. Til dæmis er hún þátttakandi í norrænu samstarfi CERT-netöryggissveita um gagnkvæm upplýsingaskipti, þar sem skipst er á margs konar gögnum um öryggisógnir, varnir og viðbúnað. Ennfremur fylgist hún með ógnum og öryggisatvikum samkvæmt samstarfssamningum við ýmsa innlenda og erlenda aðila.

2. Efling þekkingar

Sveitin veitir almennar upplýsingar um aðgerðir og viðbúnað þegar svo ber undir.

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.

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.

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.

Síendurtekin atvik sem sveitin fékkst við á árinu 2014

DDoS árásir á fjarskiptafyrirtæki

Óprúttnir aðilar gerðu DDoS árásir á fjarskiptafyrirtæki og banka hérlendis. Hver undirrótin var er ekki ljóst en þessar árásir voru gerðar í nokkur skipti og var brugðist skjótt við af þeim sem fyrir þeim urðu. Komu þá að góðum notum æfð vinnubrögð í svona málum. CERT-ÍS var að mestu á hliðarlínunni enda hefur sveitin almennt ekki beina aðkomu að slíkum málum, en veitir ráðgjöf og aðra aðstoð ef eftir því er leitað. Sömuleiðis efndi hún til samráðs með stærri hópi sem tengdist þessum atvikum til að fá fram stöðu annarra og samstöðu um hvernig best væri að bregðast við. Sveitin gaf einnig út leiðbeiningar fyrir minni fyrirtæki til að bregðast við DDoS árásum. Bæklinginn er að finna á heimasíðu sveitarinnar www.cert.is.

Phishing árásir á fjarskiptafyrirtæki og banka

Nokkrir bankar og a.m.k. eitt fjarskiptafyrirtæki urðu fyrir síendurteknum Phishing árásum á árinu. Tilgangurinn virtist vera að komast yfir aðgangsupplýsingar viðskiptavina þessara aðila, en yfirleitt er tilgangurinn með slíkum árásum að komast yfir fjármuni. Hér gilti það sama og varðandi DDoS árásirnar sem nefndar voru hér á undan, að vel samhæfð vinnubrögð milli viðkomandi skotmarka og fjarskiptafyrirtækja, sem og skjót upplýsingaskipti, komu því til leiðar að hægt var að loka á viðkomandi vefslóðir.

Erlent samstarf

Erlent samstarf er lykill að rekstri netöryggissveita. Sveitirnar hafa ákveðið samskiptalag á heimsvísu, þar sem þær skiptast á ýmsum upplýsingum og ráðgjöf.

Alþjóðlegt samstarf netöryggissveita er jafnframt mikilvægt til að samræma aðgerðir og gera viðbúnað og viðbrögð sem skilvirkust.

Norrænt samstarf

Varðandi alþjóðlegt samstarf leggur CERT-ÍS mesta áherslu á samstarf við hin Norðurlöndin. Nú þegar eru þau tengsl orðin það góð að við getum leitað þangað með vandamál og fengið ráðgjöf ef svo ber undir. Norðurlöndin sem ein heild eru öflug eining þegar kemur að vernd netheima, og þar leggjum við okkar af mörkum með þátttöku í sameiginlegum stýrifundum, umfjöllun sérfræðinga o.s.frv. Hins vegar erum við á eftir þeim með að tengjast inn á öryggisvottað (classified) upplýsingaskiptanet norrænu CERT sveitanna.

Almenn er norrænt samstarf mjög ofarlega í forgangi hérlendis og í netöryggismálum grundvallast það 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. Okkar þáttur í þessu verkefni hefur dregist af ýmsum orsökum. Upplýsingaskiptanetið er nauðsynlegt tól fyrir gagnkvæm upplýsingaskipti, þar sem skipst er á margs konar gögnum um öryggisatvik, varnir og viðbúnað. Búið er að kaupa sérhæfðan öryggisvottaðan búnað til að gera þetta kleift en því miður hefur ekki tekist að útvega öryggisvottað rými til að hýsa búnaðinn. Slíkt rými kostar fé til að sinna þeim miklu öryggiskröfum sem um slíkt rými gildir. Póst- og fjarskiptastofnun er ekki tilbúin í að leggja í þann kostnað á meðan óvissa ríkir um staðsetningu sveitarinnar til framtíðar. Mál þetta er eitt af nokkrum sem hefur ekki komist á skrið vegna óvissunnar um flutning sveitarinnar til almannavarnardeildar RLS.

Hið norræna samstarf er því, enn sem komið er, byggt á funda- og umræðugrundvelli auk þess sem sameiginlegar æfingar eru í bígerð. Má geta þess að hinar þjóðirnar hafa gengið frá sínum tengingum inn á upplýsingaskiptanetið. Það að við skulum ekki vera þeim samstíga er farið að skapa ákveðið vandamál í samstarfinu. Til dæmis um slíkt er að við fáum ekki tilkynningar um það sem sent er um netið en þar eru oft á ferðinni upplýsingar sem gætu skipt okkur töluverðu máli.

Samstarf við ENISA

Sem fyrr hefur Póst- og fjarskiptastofnun gott samstarf við Net- og upplýsingaöryggisstofnun Evrópusambandsins, ENISA, ekki síst um CERT málefni, málefni ómissandi upplýsingainnviða, um stefnu ESB í netöryggismálum o.fl. Er þessi samvinna eitt af forgangsverkefnum CERT-ÍS, næst á eftir Norðurlandasamstarfinu, enda nýtist þaðan mikil reynsla og þekking á þessu sviði.

Vaxandi ógnir og önnur mál

Mikil umfjöllun hefur verið erlendis á árinu um margskonar ógnir gagnvart netöryggi, svo sem dulkóðunartækni sem hefur verið brotin upp, stærri og dreifðari DDoS árásir hafa verið gerðar en áður, uppljóstranir og njósnamál eru í algleymingi sem og fréttir af hlerunum, árásir eru gerðar milli ríkja, aðgerðir aðgerðarsinna hafa verið áberandi, aukin gagnagíslataka, upplýsingastuldur og pólitískar tölvuárásir hafa verið í fréttum o.s.frv.

Vaxandi skilningur er almennt á þörfinni fyrir eflt netöryggi en leggja þarf áherslu á vitundarvakningu og fræðslu um hvernig fólk getur varið sig og gögn sín.

Sem fyrr þurfa netöryggisaðilar stöðugt að uppfæra þekkingu sína og vera á varðbergi gagnvart nýjungum á sviði netógna.

Svokölluð gagnagíslataka (e. ransom-ware) , er eitt form fjárkúgana sem 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 notkun tölvuskýja og skýjaþjónustu ýtir undir að aðilar móti sér stefnu um hvort og þá hvernig þeir skuli haga sínum málum í þeim efnum.

Mikilvægt er að fyrirtæki sem nota SCADA kerfi sem eru notuð til að stjórna ýmsum búnaði í iðnaði, við raforkuframleiðslu o.s.frv., hugi vel að öryggi kerfanna í ljósi þess að ógnir sem steðja að þeim fara sífellt vaxandi.

Starfsáætlun fyrir 2014 og framvinda hennar

Í starfsáætlun fyrir síðasta ár var lögð áhersla á nokkur verkefni í starfi CERT-ÍS og er hér á eftir farið stuttlega yfir hver framvinda þeirra var.

- ✓ 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.
  Þetta mál náðist að hluta til en tæknilegir örðugleikar urðu þess valdandi að ekki var hægt að ljúka verkefninu að fullu.
- ✓ Enn meiri áhersla á sameiginlegar æfingar, svo sem sameiginlega æfingu netöryggissveita Norðurlandanna, CE-2014.
  Þetta gekk vel eftir með sameiginlegum undirbúningi fyrir norrænu æfinguna sem áætluð er í byrjun árs 2015, sem og undirbúningsþátttaka vegna CE-2014. En þegar upp var staðið tók sveitin aðeins þátt í fyrsta hlutanum af þremur.
- ✓ Sérstökum samráðsvettvangi komið á um stærri mál sem kunna að koma upp.
  Þetta gekk eftir í nokkrum málum en gera þarf betur á næstu árum.
- ✓ Endurbætur í kjölfar Vodafone málsins
  Ýmsir verkferlar hafa verið teknir til endurskoðunar, sem og að skerpa á fókus sveitarinnar á ógnir sem ógna ómissandi upplýsingainnviðum Íslands.
- ✓ Útvíkkun þjónustuhóps sveitarinnar
  Þetta gekk ekki eftir, aðallega vegna þeirrar óvissu og losaragangs sem var í kringum áætlanir um flutning á sveitinni, sem síðan varð ekki af.

- ✓ Efla og prófa reglulega gæði sveitarinnar er lýtur að innri málum, svo sem verkefnum og verkferlum, þjálfun starfsmanna o.s.frv.
  Sveitin vann vel að þessum málum miðað við aðstæður og er þetta í raun síverkefni sem alltaf er gott að endurskoða og gera betur.

Í starfsáætlun sveitarinnar á árinu 2015 verður meðal annars lögð áhersla á eftirfarandi atriði:

- ✓ Forgangsröðun þjónustu og samstarfs í samræmi við getu og fjármagn sveitarinnar
- ✓ Betri nýting á vefgátt og upplýsingaskiptakerfi við þjónustuhópinn
- ✓ Áhersla á sameiginlegar æfingar, eins og kostur er.
- ✓ Verkferlar verði endurbættir
- ✓ Verkferlar til að nota í netkrísum verði gerðir
- ✓ Áhersla á þekkingu og viðbúnað varðandi netöryggi SCADA kerfa hérlendis
- ✓ Efla gangverk fyrir tilkynningar til CERT-ÍS um öryggisatvik hérlendis
- ✓ Sérstakur samráðsvettvangur um ýmiss stærri mál verði efldur
- ✓ Útvíkkun þjónustuhóps sveitarinnar
- ✓ Gæði í innra starfi sveitarinnar, svo sem verkefnum og verkferlum, þjálfun starfsmanna o.s.frv., verði áfram efld og prófuð reglulega. *
- ✓ Geta og þekking sveitarinnar til að taka á APT ógnum verði efld