ÁRSSKÝRSLA CERT-ÍS 2016

PÓST- OG FJARSKIPTASTOFNUN

Efnisyfirlit

Inngangur

Skýrsla sú sem hér birtist er fjórða ársskýrslan sem netöryggissveitin CERT-ÍS sendir frá sér. Henni er sem fyrr ætlað að veita innsýn í starfsemi og verkefni sveitarinnar á liðnu ári, nú vegna ársins 2016.

Netöryggissveitin CERT-ÍS, stefnumótun og þróun sveitarinnar

Í byrjun árs 2016 setti innanríkisráðuneytið á stofn verkefnið *Mótun heildarskipulags netöryggissveita á Íslandi.* Verkefnið hafði nokkur meginmarkmið en hér fyrir neðan eru talin þau sem CERT-ÍS hafði beina aðkomu að:

Samfélagslegt markmið:
Að efla net- og upplýsingaöryggi mikilvægra innviða samfélagsins.

Verkefnaleg markmið:

1. Koma með fyrir 15. janúar 2016 tillögur um úrbætur hjá CERT-ÍS til þess að netöryggissveitin geti sinnt lögboðnum skyldum sínum og boðið CERT-teymum atvinnugreina þjónustu á grunni þjónustusamninga.
2. Móta drög að innihaldi þjónustusamninga milli CERT-ÍS og annarra CERT-teyma fyrir 5. febrúar 2016 og stuðla að því að slíkir samningar yrðu gerðir fyrir 1. maí 2016.
3. Móta tillögu um GovCERT í samvinnu við hlutaðeigandi ráðuneyti, skipulag og verkefni með hliðsjón af heildarskipulagi CERT-mála (sbr. 2 lið) fyrir 12. febrúar 2016 og að það teymi gæti orðið starfhæft 1. maí 2016.

Netöryggissveitin vann að ákveðnum þáttum verkefnisins í góðri samvinnu við ráðuneytið á árinu og náðist góður árangur í flestum þessum þáttum þó vinnunni væri ekki lokið um áramót. Sveitin skilaði tillögum að úrbótum sem nauðsynlegar eru til þess að CERT-ÍS geti sinnt sínum skyldum. Meginþættir tillagnanna voru um þörf á endurnýjun á upplýsingatæknibúnaði sveitarinnar ásamt því að finna hentugt húsnæði fyrir starfsemina og því að geta tekið í notkun samnorrænan samskiptabúnað sem sveitin á en krefst sérhæfðs og vottaðs umhverfis. Á vormánuðum 2016 veitti fjarskiptasjóður netöryggissveitinni styrk til þess að endurnýja upplýsingatæknikerfi sín og fljótlega fór af stað vinna við að að finna hentuga starfsaðstöðu fyrir sveitina.

Síðsumars kom upp sú hugmynd milli lögreglunnar á höfuðborgarsvæðinu (LRH) og Póst- og fjarskiptastofnunar (PFS) um aukið samstarf þessara aðila á sviði netöryggismála og rannsókna á atvikum sem upp koma á sviði netöryggismála hjá þeim. Strax lá fyrir vilji beggja um að skapa grundvöll fyrir sameiginlegri starfsaðstöðu þannig að CERT-ÍS flytti starfsemi sína og tækjabúnað í húsnæði LRH að Vínlandsleið 2-4. Á frumstigum var þetta skoðað sérstaklega af innanríkisráðuneytinu og með stuðningi og ákvörðun þess er samstarfið orðið að veruleika. Var sveitin flutt um mitt ár 2017. Samhliða þessari vinnu var metin þörf beggja aðila til endurnýjunar upplýsingakerfa þeirra og hugsanleg samlegð varðandi innkaup og rekstur þeirra. Sú vinna er enn í gangi.

Þá vann CERT-ÍS að því með ráðuneytinu að móta drög að þjónustusamningi milli CERT-ÍS og annarra CERT-teyma hérlendis og hafa þau drög verið kynnt fjármálageiranum og orkugeiranum til skoðunar með fyrirhugaðan samstarfssamning í huga. Áfram er unnið af hálfu ráðuneytisins að því að móta tillögu að stofnun GovCERT.

Við árslok 2016 var heildarstarfsmannafjöldi netöryggissveitarinnar tveir starfsmenn. Vonir standa til að þeim muni fjölga í takti við að samningar verði gerðir við aðila mikilvægra innviða samfélagsins.

Yfirlit 2016

Á árinu 2016 vann netöryggissveitin CERT-ÍS markvisst að uppbyggingu á getu og þekkingu varðandi kjarnahlutverk sitt. Þjóðar-CERT, eins og CERT-ÍS, hafa ýmsum skyldum að gegna varðandi þjónustuhóp sinn og hefur verið byggt upp öflugt samstarf við fjarskiptageirann, sem er skilgreindur þjónustuhópur CERT-ÍS samkvæmt núgildandi regluverki. Þess ber þó að geta að sveitin hefur einnig átt gott samstarf við aðra innlenda geira og lögð er áhersla á að aðstoða eftir föngum við verkefni sem geta haft áhrif á mikilvæga upplýsingainnviði þjóðarinnar.

Atvik ársins

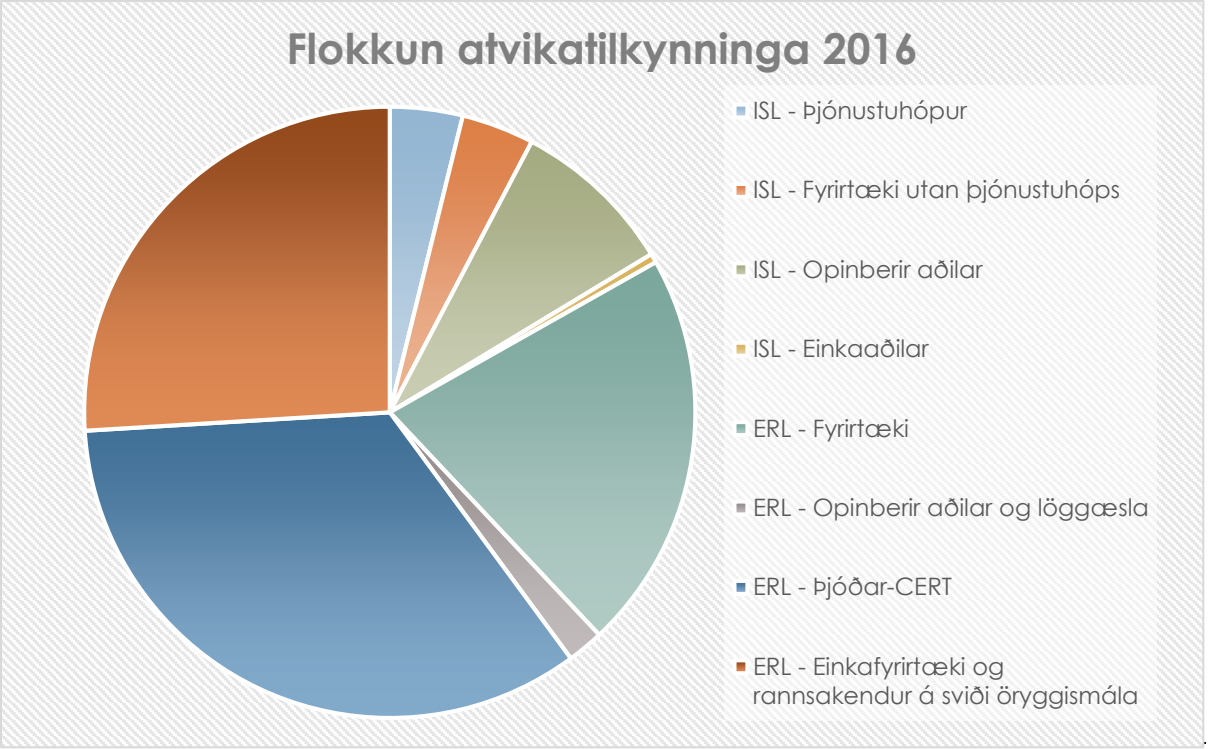
CERT-ÍS meðhöndlar atvikatilkynningar frá öllum aðilum, án tillits til þess hvort sá sem tilkynnir er í skilgreindum þjónustuhópi sveitarinnar. Tilkynningar eru metnar og forgangsraðað með tilliti til þess hvort þær falla undir skilgreint starfssvið sveitarinnar samkvæmt reglugerð um starfsemi hennar. Atvikamál eru síðan stofnuð á grundvelli tilkynninga ef tilefni er til. Atvikatilkynningar eru mikilvægt innlegg í mótun á stöðumynd fyrir netlögsöguna og því nauðsynlegt að gera átak í að fjölga innlendum tilkynningum til að sú mynd geti orðið sem skýrust. Má nefna að talsvert var um atvikatilkynningar frá netstjórum innlendra fyrirtækja og stofnana sem byggðu á skýrslum úr varnarbúnaði á netlagi eða endabúnaði þeirra. Þessar tilkynningar reyndust vera innlegg í úrlausn mála sem vörðuðu þjóna sem dreifðu spillikóða til endanotenda.

Alls bárust CERT-ÍS 208 atvikatilkynningar og erindi varðandi skilgreind atvik á árinu. Atvikatilkynningar frá innlendum aðilum voru 35 en 173 frá erlendum aðilum. Nánar má sjá flokkun tilkynnenda í töflu 1 og mynd 1 hér fyrir neðan. Þess ber að geta að grundvöllur tölfræðinnar er lítillega breyttur frá því sem var starfsárið 2015 og samanburður varðandi fjölda skráðra atvikatilkynninga og atvika milli ára því ekki fyllilega marktækur. Sjá má að meirihluti atvikatilkynninga berst frá erlendum aðilum og varða í raun í tiltölulega fáum tilvikum núverandi þjónustuhóp sveitarinnar, sem samkvæmt gildandi regluverk eru skráð fjarskiptafélög. Sem þjóðartengiliður í netöryggismálum ber CERT-ÍS sem þjóðartengiliði í netöryggismálum að meðhöndla tilvik þar sem innlendir aðilar eru taldir brjóta, viljandi eða óviljandi, á erlendum fyrirtækjum eða einstaklingum. Skylda CERT-ÍS í slíkum tilvikum er að upplýsa aðila sem eru til þess færir að leysa úr viðkomandi máli og reynast slík verkefni stór hluti af daglegum viðfangsefnum sveitarinnar.

Alls voru 147 atvikamál skráð og meðhöndluð af CERT-IS á grundvelli atvikatilkynninga árið 2016. Nánari greiningu á atvikum er að finna í töflu 2 og mynd 2. Einnig er gerð grein fyrir helstu flokkum atvika hér að neðan.

Tafla 1: Atvikatilkynningar skráðar árið 2016

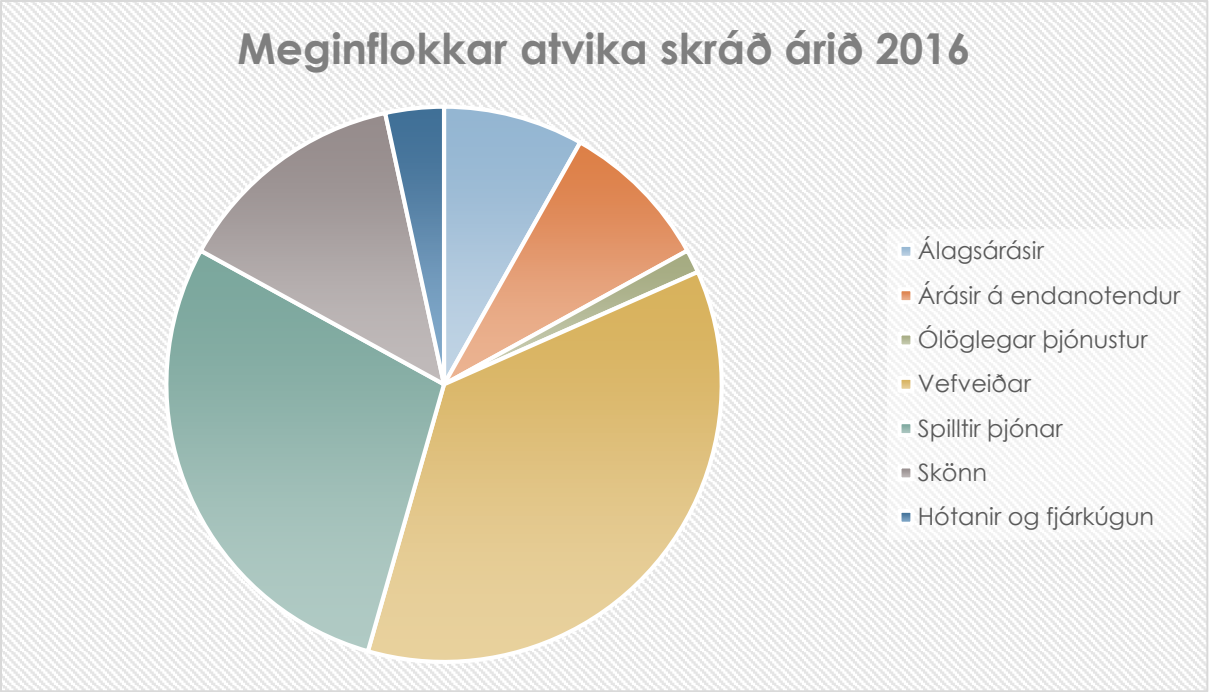
Þjóðerni	Flokkur	Fjöldi
ISL	Þjónustuhópur	8
ISL	Fyrirtæki utan þjónustuhóps	8
ISL	Opinberir aðilar	18
ISL	Einkaaðilar	1
ERL	Fyrirtæki	44
ERL	Opinberir aðilar og löggæsla	4
ERL	Þjóðar-CERT	71
ERL	Einkafyrirtæki og rannsakendur á sviði tölvuöryggis	54



Mynd 1: Flokkun aðila sem tilkynntu atvik - atvikatilkynningar skráðar árið 2016

Tafla 2: Helstu flokkar atvika sem stofnuð voruð árið 2016

Flokkar atvika	Fjöldi
Álagsárásir – DoS, DDoS, mögnunarárásir	12
Árásir á endanotendur og spillibúnaður	13
Ólöglegar þjónustur	2
Vefveiðar og svikapóstar	53
Spilltir þjónar	42
Skönn og könnunaraðgerðir	20
Hótanir og tilraunir til fjárkúgunar	5



Mynd 2: Helstu flokkar atvika sem skráð voru árið 2016

Álagsárásir

Markmið álagsárása er að stöðva eða takmarka afkastagetu þeirra sem fyrir þeim verða. Oft er um að ræða sk. dreifðar álagsárásir (DDoS) sem framkvæmdar eru með aðstoð stórra botneta. Aðkoma CERT-ÍS að slíkum málum er almennt ráðgefandi en einnig er fylgst með hvort íslenskir aðilar taka þátt í slíkum árásum. Til þessa hefur verið lítið um slíkt en þarf þá einnig að taka tillit til þess að tilkynntar álagsárásir eru enn sem komið er fáar. Þar sem um hefur verið að ræða íslenska gerendur er í nær öllum tilvikum um að ræða veikleika, s.s. DNS veikleika, sem nýttir eru til umferðarmögnunar af erlendum aðilum.

Árásir á endanotendur

Nokkuð var um tilkynningar atvika sem vörðuðu endanotendur. Til slíkra atvika teljast tilkynningar um sýkingar af ýmsu tagi og tilkynningar um leka persónuupplýsinga. CERT-ÍS leitast við að gefa þeim tilkynnendum sem hafa samband við sveitina ráð varðandi sýkingar í kerfum þeirra. Einnig er talsvert um tilkynningar frá erlendum samstarfsaðilum sem greina vísbendingar um sýkingar og tilkynna til CERT-ÍS. Í þeim tilvikum er leitast við að upplýsa viðkomandi notendur en það getur reynst torvelt. Núverandi regluverksumhverfi heimilar CERT-ÍS ekki að óska persónuupplýsinga um endanotendur frá fjarskiptafélögum. Eina leið sveitarinnar er því oftast að koma upplýsingum á framfæri við fjarskiptafélögin og biðja þau um að upplýsa viðskiptavini sína. Mikill meirihluti fjarskiptafyrirtækja er þó reiðubúinn að koma slíkum upplýsingum áfram. Þess ber að geta að lítið er um að innlendir endanotendur tilkynni öryggisatvik til CERT-ÍS.

Þá komu einnig upp tilvik þar sem tilraunir voru gerðar til gagnagíslatöku hjá fyrirtækjum og einstaklingum. Aðkoma CERT-ÍS að slíkum málum er fyrst og fremst að upplýsa um fyrirbyggjandi aðgerðir. Áhersla hefur verið lögð á að fyrirtæki sem og einstaklingar gæti þess að taka afrit af gögnum, sjái til þess að vera með nýjustu útgáfur af hugbúnaði og að notendur gæti þess að smella

ekki á slóðir eða opni skjöl frá aðilum sem ekki eru þekktir. Tiltölulega fáar gagnagíslatökur voru tilkynntar til CERT-IS starfsárið miðað við umfang slíkra árása á heimsvísu og má leiða líkur að því að þær snerti í fæstum tilvikum þjónustuhóp sveitarinnar.

Ólöglegar þjónustur

Örfá tilvik hafa verið flokkuð af CERT-ÍS sem ólöglegar eða óheimilar þjónustur. Um getur verið að ræða þjónustur sem miðla höfundarréttarvörðu efni, auglýsa vopn, fíkniefni eða stolnar upplýsingar s.s. kreditkortanúmer. CERT-ÍS meðhöndlar ekki slík mál, umfram að skrá og flokka, en vísar þeim til meðferðar hjá lögreglu.

Vefveiðar og svikapóstar

Eins og fyrri ár hafa vefveiðar af ýmsu tagi verið stærsti einstaki flokkur atvika sem skráð eru hjá CERT-ÍS. Atvik í þessum flokki eru í langflestum tilfellum falskar vefsíður, eða 43 af alls 53 skráðum atvikum. Einnig er nokkuð um tilkynningar sem varða tölvupósta sem vísa á falssíður. Er þá um að ræða vefsíður sem líkja eftir raunverulegum vefsíðum fyrirtækja með það fyrir augum að veiða persónuupplýsingar notenda s.s. notendanöfn, lykilorð og kortanúmer. Í flestum tilvikum er um að ræða erindi frá erlendum aðilum varðandi svikaþjóna sem settir eru upp hérlendis en einnig kemur fyrir að innlendir aðilar kvarta undan þjónum sem beinast gegn þeim og hýstir eru erlendis. Í þessum tilvikum leitast CERT-ÍS við að stöðva starfsemina í samvinnu við eigendur og hýsingaraðila, en þess má geta að oftast er um að ræða vefþjóna sem hefur verið spillt af tölvuþrjótum og svikastarfsemin því ekki á vegum raunverulegra eigenda. Einnig er rétt að geta þess að engin lagaskylda hvílir á hýsingaraðilum að sinna samstarfi við CERT-ÍS í tilvikum sem þessum og hefur sú aðstaða komið upp að ekki er unnt að bregðast við atviki vegna þess að hýsingaraðili sinnti ekki tilmælum CERT-ÍS.

Spilltir þjónar

Annar stærsti flokkur atvika ársins varðar spillta netþjóna sem geta skaðað notendur. Þar er m.a. um að ræða sk. „exploit kit“ þjóna og stjórnþjóna slíkra kerfa sem sett eru upp með það markmið að lauma spillikóða af ýmsu tagi til endanotenda. Er þar m.a. um að ræða búnað til að stela persónu-upplýsingum og gagnagíslatökubúnað. Tilkynningar um grunaða þjóna bárust bæði frá innlendum og erlendum aðilum. Erlendir samstarfsaðilar finna oft ummerki sem benda til spillingar á sínum gögnum og koma þeim þá til skila við viðkomandi þjóðar-CERT. Einnig hafa mikilvægar upplýsingar borist frá íslenskum kerfisstjórum sem sjá ummerki um slíkan búnað í sínum varnarkerfum. CERT-ÍS hefur lagt áherslu á að grafast fyrir um atvik af þessu tagi og unnið náið með eigendum og ábyrgðaraðilum til að hreinsa sýkta þjóna.

Skönn og könnunaraðgerðir

Nokkuð er um að tilkynnt sé til CERT-ÍS um skönn og könnunaraðgerðir á kerfum, s.s. portskannanir, veikleikaskannanir og tilraunir til aðgangs að kerfum með þekktum lykilorðalistum. Oftast er um að ræða sjálfvirkar skýrslur frá varnarkerfum erlendra aðila sem fyrir slíku verða. CERT-ÍS bregst almennt ekki við könnunaraðgerðum nema þær beinist gegn íslenskum aðilum í þjónustuhópi eða þeim sem teljast til mikilvægra upplýsingainnviða. Oft eru þær könnunaraðgerðir sem raktar eru til IP talna í íslensku netlögsögunni frá sk. nafnleyndarþjónustum, svo sem VPN útgangspunktum, og því nær ómögulegt að rekja til raunverulegra gerenda.

Hótanir og tilraunir til fjárkúgunar

Fimm atvik voru skilgreind sem hótanir og tilraunir til fjárkúgunar. Í öllum tilfellum var um að ræða hótanir um DDoS árás gegn lausnargjaldi í bitcoin. Aðkoma CERT-ÍS að slíkum málum er fyrst og fremst að upplýsa aðra aðila í þeim geira sem hótunin beinist gegn og fylgjast með þróun mála. Í engu tilfella ársins 2016 reyndist um að ræða alvarlega hættu tengda slíkum hótunum, en nokkrar litlar sýniárásir geta hafa tengst þeim. Þær sýniárásir voru almennt ekki skráðar sem sérstök atvik árið 2016.

Viðbragðsáætlun og netæfing

Viðbragðsáætlun þjónustuhóps CERT-ÍS, unnin í samstarfi CERT-ÍS og fulltrúa fjarskiptafélagana, var gefin út til þjónustuhópsins haustið 2016. Viðbragðsáætluninni er ætlað að vera leiðbeinandi skjal sem fjarskiptafélögin geta beitt við mótun innri áætlana sinna og verður hún uppfærð reglulega. Í framhaldi af útgáfu fyrstu draga viðbragðsáætlunarinnar var haldin netæfing CERT-ÍS og fjarskiptafélaganna þann 22. nóvember 2016. Æfingin var haldin í húsakynnum almannavarna í Skógarhlíð í Reykjavík og í henni tóku þátt fulltrúar stærstu fjarskiptafélaganna. Tilgangur æfingarinnar var fyrst og fremst að þjálfa boðleiðir milli aðila í umfangsmiklum neyðartilvikum. Gekk æfingin vel og þjónaði því hlutverki sínu. Ætlunin er að halda slíka æfingu annað hvort ár.

Samstarf

CERT-ÍS á sæti í netöryggisráði og á þar samstarf með lykilaðilum varðandi upplýsingaöryggi landsins. CERT-ÍS hefur einnig haldið áfram að rækta samstarf sitt við norrænu netöryggissveitirnar í sk. Nordic CERT Cooperation (NCC) samstarfi. Í því eiga sæti fulltrúar Norðmanna, Dana, Svía og Finna auk Íslendinga. Einnig var stofnað til náins samstarfs varðandi þróun og fræðslu við CERT-SE, sem er þjóðar-CERT Svíþjóðar.

Þjónustuhópur CERT-ÍS samkvæmt regluverkinu eru fyrirtæki á fjarskiptamarkaði á Íslandi. Samstarf við þjónustuhópinn var eflt verulega á árinu þegar teknir voru upp mánaðarlegir fundir á samráðsvettvangi aðila eins og heimild er fyrir í reglugerðinni. Einnig voru stofnaðir vinnuhópar CERT-ÍS og þjónustuhópsins sem ætlað er að leggja línur í samskiptum milli aðila, auk smíði viðbragðsáætlunar og undirbúnings netæfingar eins og áður var nefnt.

Fyrstu skref til nánara samstarfs við íslenska löggæslu voru stigin á árinu þegar viðræður hófust um sameiginlegt húsnæði og aukið daglegt samstarf við lögregluna á höfuðborgarsvæðinu. Var gengið frá samningsdrögum um aðild Póst og fjarskiptastofnunar/CERT-ÍS að hópi löggæsluaðila sem starfa að net og tölvurannsóknum í desember 2016. Einnig tóku CERT-ÍS og lögreglan á höfuðborgarsvæðinu þátt í ráðstefnu ENISA og EUROPOL/EC3 í Haag um málefni er varða samvinnu CERT og löggæsluaðila um netöryggismál og netglæpi.

Þjónustusamningar

Innanríkisráðuneytið ákvað, árið 2015, að falla frá áformum um nýja lagasetningu um málefni CERT-ÍS og þar með talið áformum um lögbundna stækkun þjónustuhópsins. Þess í stað var kveðið á um að CERT-ÍS myndi nýta heimildir í núverandi reglugerð 475/2013 sem kveða á um að CERT-ÍS megi stækka þjónustuhóp sinn með gerð þjónustusamninga. Vinna við undirbúning slíkra þjónustusamninga hófst í upphafi árs 2016 með þátttöku í samstarfsverkefni með innanríkisráðuneyti um framtíðarskipulag CERT mála á Íslandi. Í árslok 2016 var grundvöllur samninga orðinn skýr og standa vonir til að fyrstu þjónustusamningarnir verði gerðir árið 2017.

Aukið samstarf við löggæslu

Haustið 2016 hófust óformlegar viðræður um aukið samstarf milli CERT-ÍS og löggæsluaðila á sviði tölvubrota. Í lok ársins var gengið frá samkomulagi um að CERT-ÍS yrði aðili að hópi sem þegar eru í rannsakendur á sviði tölvubrota frá lögreglunni á höfuðborgarsvæðinu, embætti ríkislögreglustjóra, lögreglunni á Suðurnesjum og embætti saksóknara. Samhliða þessu var ákveðið að CERT-ÍS myndi flytja starfsstöð sína að Vínlandsleið í Reykjavík, þar sem tölvurannsóknadeild LRH hefur aðsetur. Áætlað er að starfsstöðin verði tekin í notkun um mitt ár 2017.

Uppbygging upplýsingakerfa

Í upphafi árs 2016 var ljóst að gera þurfti átak í endurnýjun upplýsingakerfa netöryggissveitarinnar, þar á meðal vélbúnaðar. Í samvinnu við innanríkisráðuneytið var gerð úttekt á þörfinni hvað þetta varðar og í framhaldi af því var veitt fjármagn úr fjarskiptasjóði til verkefnisins. Í tengslum við formlegt samstarf CERT-ÍS og löggæsluaðila hófust viðræður um sameiginlegan rekstur tölvukerfa þessara aðila. Fyrstu skrefin varðandi áætlanir voru tekin í lok árs 2016 og stendur til að gagnger endurnýjun á rekstrarumhverfi upplýsingakerfa sveitarinnar hefjist um mitt ár 2017. Sú breyting mun hafa í för með sér verulegt hagræði og aukið rekstraröryggi fyrir starfsemi CERT-ÍS.

Innleiðing á nýju upplýsingakerfi, sem heldur utan um sjálfvirkar upplýsingaveitur sem sveitin hefur aðgang að, hófst haustið 2016. Um er að ræða upplýsingar sem berast frá ýmsum aðilum á sviði upplýsingaöryggis, bæði opnar upplýsingar (OSINT) og upplýsingar sem eru takmarkaðar við CERT sveitir og samstarfsaðila þeirra. Tilraunakeyrsla kerfisins hófst í lok árs 2016 og tók það við að meðaltali um 1.000 stökum atburðatilkynningum á dag. Atburður telst hér hver einstök vísbending um veikleika eða misnotkun sem rekja má til íslenskra IP talna, en oft er sama atburð að sjá í straumum fleiri en eins tilkynnanda. Séu einungis taldir þeir atburðir sem hugsanlega varða alvarlegri tilvik, s.s. botnet þjóna, reyndust þeir taldir í tugum daglega en þó ber að taka tillit til þess að sama sýkingartilvik getur borist í gagnastraumum síendurtekið yfir nokkurra daga tímabil. Árið 2016 einskorðaðist vinnsla þessara gagna að mestu við tölfræðilega úrvinnslu en árið 2017 mun verða unnið úr þeim á markvissari hátt með það að markmiði að bæta ástand íslensku netlögsögunnar. Er þá bæði ætlunin að ráðast í afmörkuð átaksverkefni til að bæta úr útbreiddum veikleikum og stofna í ríkara mæli atvikamál að eigin frumkvæði sveitarinnar til að takast á við alvarlegri sýkingatilfelli.

Starfsáætlun CERT-ÍS fyrir árið 2017

Í starfsáætlun netöryggissveitarinnar CERT-ÍS fyrir árið 2017 er meðal annars lögð áhersla á eftirfarandi:

- Áframhaldandi uppbyggingu á samstarfi við þjónustuhóp sveitarinnar sem felst m.a. í samvinnu um mótun verklags aðila varðandi viðbrögð við atvikum
- Stækkun þjónustuhóps með gerð þjónustusamninga við rekstraraðila mikilvægra upplýsingainnviða
- Aukna samvinnu við erlendar CERT sveitir sem og löggæslu hérlendis og erlendis

- Aðkomu að mótun lagaumhverfis um net og upplýsingaöryggi á Íslandi m.a. með tilliti til aðstæðna í Evrópu.
- Eflda meðhöndlun atvika, m.a. að nýttar verði að fullu þær upplýsingar um atvik sem berast frá erlendum upplýsingaveitum. Einnig verði upplýsingar um veikleika nýttar til að ráðast í afmörkuð átaksverkefni til að bæta ástand netlögsögunnar.
- Uppbyggingu á starfsstöð og upplýsingakerfum sveitarinnar
- Menntun og þjálfunarmál, m.a. námskeið og heimsóknir til erlendra systurstofnana
- Þátttaka í innleiðingu tilskipunar ESB um netöryggi, svo kallaða NIS tilskipun, en ráðgert er að innleiða hana í íslensk lög árið 2018. Með henni er settur mun skýrari og umfangsmeiri starfsumgjörð um starfsemi netöryggissveita á EES svæðinu.