ÁRSSKÝRSLA CERT-ÍS 2015

stefan.st

PÓST- OG FJARSKIPTASTOFNUN

Efnisyfirlit

Frá hópstjóra sveitarinnar

Skýrsla sú sem hér birtist er þriðja 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 2015.

Netöryggissveitin CERT-ÍS

Ýmsar hugmyndir voru uppi á árinu 2015 er sneru að framtíð sveitarinnar og framtíðarhlutverki hennar. Sumar þeirra erfðust frá fyrra ári og ein þeirra var sú að færa skyldi sveitina frá Póst- og fjarskiptastofnun (PFS) til embættis ríkislögreglustjóra (RLS). Rétt undir lok ársins 2015 var ljóst af hálfu innanríkisráðuneytisins að af því yrði ekki, heldur skyldi nota núverandi lagaheimildir hennar til að efla starfsemina með samningum við rekstraraðila svokallaðra ómissandi upplýsingainnviða.

Í ljósi þessarar stöðu sveitarinnar er nú unnið að því að nýta sem best það sem sveitin hefur við núverandi aðstæður, svo sem aðföng og annað. Þó er ljóst að að fjárheimildir sveitarinnar í dag rúma ekki nauðsynlega þætti í starfsemi hennar.

Við stofnun sveitarinnar hófu þrír starfsmenn störf. Einn hætti síðari hluta árs 2014, annar á sumarmánuðum 2015 og aðeins einn var ráðinn í stað þessara tveggja.
Sveitin samanstendur því af tveimur föstum starfsmönnum í stað þriggja eins og var við stofnun hennar. Þegar ljóst var að af flutningi til RLS yrði ekki, var ákveðið að forstöðumaður tæknideildar PFS kæmi meira inni í dagleg málefni sveitarinnar.

Við árslok 2015 var því heildarstarfsmannafjöldi netöryggissveitarinnar áfram tveir. Það má telja of lítið fyrir núverandi starfsemi, sveitin þyrfti að hafa að lágmarki fjóra starfsmenn til sinna hlutverki sínu og þróa starfsemina áfram.

Starfsemin

Í störfum sínum einbeitir sveitin sér mest að kjarnaþjónustuhópi sínum, sem ennþá er eingöngu þau fjarskiptafyrirtæki sem greiða hlutafall af veltu sinni til rekstursins. Sem netöryggissveit á landsvísu og tengiliður Íslands út á við gagnvart erlendum CERT hópum, hefur sveitin þó víðara hlutverki að gegna. Í því kristallast mótsögn sem kemur oft upp í daglegu starfi sveitarinnar; hún er skv. lögum netöryggissveit á landsvísu en þjónustuhópurinn samanstendur af fyrrgreindum fjarskiptafyrirtækjum. Þau eru forgangsaðilar í þjónustu sveitarinnar, ásamt þeim aðilum sem mögulega gera sérstakan samning við sveitina um að koma inn í þjónustuhópinn. Þetta, ásamt óljósum heimildum sveitarinnar til að bregðast við öryggisatvikum, m.a. með því að fara fram á viðbrögð annarra, veldur oft á tíðum ómarkvissari aðgerðum en ella. Til að bregðast við þessu hyggst sveitin á nýju ári vinna nánar með þjónustuhópnum en áður, m.a. við að skipuleggja samstilltar aðgerðir, svo sem gegn þeim öryggisatvikum sem sveitin bendir fyrirtækjum á. Ennfremur þarf sveitin að fá þessa aðila til þess aðstoðar við ýmis verkefni, sem t.d. snúa að betri upplýsingamiðlun, efldu samstarfi og samhæfðum viðbrögðum gegn netvá innan þjónustuhópsins. Efla þarf samhæfingarhlutverk sveitarinnar innan netumdæmisins með markvissum upplýsingaskiptum og neyðarsamstarfi sem byggist á nýrri viðbragsáætlun sem er í undirbúningi.

Tölfræði um atvik

Á starfsárinu 2015 hófst gagnger endurskoðun og endurnýjun á upplýsingakerfum sveitarinnar. Hluti af þeirri vinnu er að skilgreina betur skráningu og utanumhald atvika, sem og tölfræðiupplýsingar

sem má greina úr þeim. Einnig stóð yfir vinna við kerfi sem safna saman upplýsingum úr þeim veitum sem sveitin hefur aðgang að. Er það von sveitarinnar að geta í framtíðinni gefið reglulega út tölfræðiskýrslur um úrlausn mála hjá sveitinni sem og almenna ástandsvitund um íslensku netlögsöguna.

Lagaumhverfi og regluverk CERT-ÍS

Í ljósi þess að ákveðið hefur verið að CERT-ÍS verði áfram hjá PFS og unnið verður að útvíkkun á starfsemi sveitarinnar, er nauðsynlegt að endurskoða lagaumhverfi það sem hún býr við. Í þessu sambandi þarf einnig að líta til breytinga sem orðið hafa í netheimum, ekki síst þegar litið er til alvarlegri ógna þar sem nauðsynlegt er að geta brugðist við á skjótan hátt. Þessi breyting á regluverkinu þarf jafnframt að taka mið af stefnu Íslands um net- og upplýsingaöryggi 2015-2026 ásamt nýrri NIS tilskipun ESB um net- og upplýsingaöryggi.

Stefna Íslands um net- og upplýsingaöryggi 2015 - 2026

Stefna Íslands um net- og upplýsingaöryggi fyrir árin 2015 - 2026 var birt um mitt árið. Átti fulltrúi sveitarinnar sæti í undirbúningsnefndinni. Þar kemur m.a. fram að efla skuli netöryggissveitina: *„Efla þarf varnir mikilvægra innviða samfélagsins. Það er fjölþætt verkefni. Öflug netöryggissveit er mikilvæg til að greina ýmsar árásir og veita aðstoð“.*

Enn fremur segir í stefnunni um vernd innviða: *„Geta netöryggissveitar til stuðla að vernd og að aðstoða mikilvæga innviði samfélagsins verði efld og virk viðbragðsgeta verði til staðar allan sólarhringinn, alla daga ársins. Sérstök áhersla verði lögð á fjarskipta-, veitu- og fjármálafyrirtæki“.*

Aðgerðaráætlun stefnunnar er fylgt eftir af netöryggisráði sem skipað er af innanríkisráðherra.

Tilskipun ESB um net- og upplýsingaöryggi handan við hornið (NIS tilskipun)

Það styttist í það að svokölluð NIS tilskipun Evrópusambandsins (Network and Information Security Directive) verði gefin út. Búið er að mestu að samþykkja textann en formlegt samþykktarferli er eftir. Þar er rætt um að hver aðildarþjóð skuli reka eina, eða fleiri, CERT sveitir sem stuðla að vernd ómissandi innviða landanna. Tryggja skal að netöryggissveit á borð við CERT-ÍS hafi næg aðföng til að sinna verkefnum sínum á skilvirkan hátt, þar með talið nægan mannskap, búnað og tækni.

Sömuleiðis er í NIS tilskipuninni rætt um mikilvægi þjóðartengiliðs hvers lands (National Single Point of Contact) í CERT málefnum. Eins og áður er getið rækir CERT-ÍS þetta hlutverk í dag og hluti af því er að vera CERT til þrautarvara þegar engin önnur úrræði eru til lausnar vissum málum. Þarf Ísland að innleiða þessa tilskipun og byrja að undirbúa hana helst á árinu 2016. Ljóst er að verulega þarf að bæta úr flestum aðföngum, aðstöðu og því umhverfi sem sveitinni er ætlað að starfa í. Reikna má með að hún taki gildi hér á landi árið 2018.

Alþjóðlegt samstarf

Nauðsynlegt er að norrænt samstarf verði eflt til mikilla muna með tengingu Íslands við öruggt upplýsingaskiptanet milli CERT sveita Norðurlandanna, þar sem þjóðirnar skiptast sín á milli á upplýsingum um netógnir og öðrum viðkvæmum upplýsingum á þessu sviði. Unnið er að því að koma upp tengingu Íslands við upplýsingaskiptanetið.

Sem þjóðartengiliður fékk sveitin eins og undanfarin ár nokkrar fyrirspurnir erlendis frá með óskum um að sveitin myndi beita sér gegn hýsingarfyrirtækjum hérlendis, sem oft eru að hýsa búnað, eða

endurhýsa búnað og veita þjónustu til annarra aðila. Eru dæmi þess að vissir aðilar kaupi slíka þjónustu hérlendis til að blekkja netverja í öðrum löndum með vefveiðum (Phishing). Mikilvægt er að Ísland taki slík mál föstum tökum eins og hægt er. Líka vegna þess að Ísland gæti þurft á slíkri aðstoð að halda í öðrum löndum.

Alvarlegar ógnir
Nokkur APT (Advanced Persistent Threats) mál komu upp á árinu. Um er að ræða „háþróaðar viðvarandi ógnir“ en vegna viðkvæmni þeirra mála sem komu upp á árinu verður ekki fjallað um einstök slík mál hér.

Æfingar og þjálfun
Á fyrstu mánuðum ársins tók sveitin þátt í samnorrænni æfingu í Svíþjóð. Var það gagnlegt en þátttaka í slíkum æfingum skilar sér alltaf vel til baka með aukinni þjálfun og þekkingu starfsmanna, ásamt betri tengslum við aðra aðila sem taka þátt.

Lokaorð
Ógnir hérlendis virðast, þegar á heildina er litið, aukast jafnt og þétt líkt og undanfarin ár og er fyrirséð að sú þróun haldi áfram.

Efla þarf samstillt átak hérlendis til að bregðast við öryggisatvikum og alvarlegri netvá. Allir þurfa að taka til í sínum ranni. T.d. er mikilvægt er að fyrirtæki sem láta sig þessi mál skipta, endurspegli vilja sinn formlega í stefnu sinni, sem og með samhliða aðgerðum, til að verja, ekki bara eigin kerfi, heldur ekki síst kerfi og búnað viðskiptavina sinna. Hér þarf að koma til töluverð hugarfarsbreyting og sömuleiðis endurskoðun á regluverkinu.

Mikilvægt er að úrræði varðandi rannsókn og meðferð mála sem snerta net og upplýsingaöryggi hérlendis verði skýrð. Hér má nefna úrræði sem varða rannsóknir alvarlegra mála (APT) þar sem í sumum tilfellum getur reynst nauðsynlegt að halda leynd gagnvart eigendum þjóna meðan gengið er úr skugga um eðli ógnarinnar og hver eru fórnarlömb árásarinnar. Einnig er nauðsynlegt að herða úrræði sem varða skyndilokanir á þjónustu sem augljóslega hýsir brotastarfsemi s.s. falsvefsíður eða dreifingu á spillikóða. CERT-ÍS vinnur nú slík mál í náinni samvinnu við löggæsluyfirvöld en nauðsynlegt er að skýra þær heimildir sem sveitin og lögregluembættin hafa til að deila upplýsingum innbyrðis sem og verklagsreglur við öflun rannsóknarúrræða.

Þjónustuveitendur geta bætt verkferla sína varðandi skyndilokanir á óæskilega þjónustu sem að ofan er rætt um. Þeir geta breytt þjónustuskilmálum með þeim hætti að vefir eða önnur þjónusta sem brýtur í bága við lög eða tilmæli CERT-ÍS sé umsvifalaust fjarlægð. Í þessu tilliti ber að geta þess að ný Evrópureglugerð (ESB) um persónuvernd var samþykkt í maí 2016 og mun formlega öðlast gildi hérlendis þann 25. maí 2018. Hún kemur til með að leggja mun ríkari ábyrgð og skyldur á þjónustu- og hýsingaraðila. Munu fyrrnefndir aðilar bera yfirábyrgð á þeirri þjónustu, þ.m.t. vinnslu persónuupplýsinga, sem er veitt og endurveitt á þeirra kerfum og netum.

Rétt er að taka fram að undir engum kringumstæðum hefur CERT-ÍS aðkomu að höfundarréttarmálum né öðrum málum en þeim sem snerta beint ógnir sem telja má að ómissandi upplýsingainnviðum stafi bein hætta af.

Er það von starfsmanna CERT-ÍS að innan úr stjórnsýslunni verði vel staðið við bakið á sveitinni og að almenningur, fyrirtæki og hið opinbera séu almennt betur að sér en áður varðandi málefni sveitarinnar og þær netógnir samtímans sem við er að glíma.

Stefán Snorri Stefánsson

Hópstjóri CERT-ÍS netöryggissveitarinnar

Yfirlit 2015

Á þessu starfsári sveitarinnar var sem fyrri ár unnið að ýmsum málum.

Daglegur rekstur

Þjóðar-CERT sveitir (e. National CERT) eins og CERT-ÍS, hafa það hlutverk að taka við erindum erlendra aðila sem hafa ekki fengið framgang sinna mála með því að leita beint til viðkomandi þjónustu- eða netveitu í landinu. Þjóðar-CERT hlutverkið felst sem sagt að hluta til í því að vera milligönguaðili sem á að ýta við „strönduðum“ málum. Oftast er ástæðan fyrir „strandinu“ sú að hérlendi aðilinn sinnir ekki erindinu, eða sinnir því seint að mati hins erlenda aðila. Þetta eitt og sér er vandamál hérlendis og bendir til að þess að bæði vanti mun samhæfðari viðbrögð og skilning veitnanna á mikilvægi þess að sinna öllum erindum eins skjótt og auðið er. Slík „strönduð“ erindi geta verið af ýmsum toga, svo sem vefveiðar (e. Phishing) t.d. þegar eftirlíking af heimasíðu banka erlendis er hýst á íslensku léni og sem torvelt reynist að loka. Eða skönnun á glufum í eldveggjum úti um allan heim er framkvæmd frá íslenskum IP tölum. Þeir sem fyrir slíku verða og telja sér ógnað kvarta oft á tíðum til CERT-ÍS.

Stefna CERT-ÍS hefur verið að vinna með þjónustuhópnum á jafnréttisgrundvelli sem byggist á velvilja og trausti fremur en að þurfa að gefa fyrirmæli. Mjög mismunandi er hvernig fyrirtæki vinna úr þessum málum. Sum þeirra hafa breytt skilmálum sínum þannig að þeim sé heimilt að láta viðskiptavin vita ef tölva hans er sýkt eða hún hluti af því sem á ensku kallast „Botnet“. Sveitin telur að persónuverndarlög styðji þetta, enda kemur eftirfarandi skýrt fram í 8. gr. laga nr. 77/2000 um persónuvernd:

- *vinnslan sé nauðsynleg til að vernda brýna hagsmuni hins skráða;*
- *vinnslan sé nauðsynleg vegna verks sem unnið er í þágu almannahagsmuna;*
- *vinnslan sé nauðsynleg við beitingu opinbers valds sem ábyrgðaraðili, eða þriðji maður sem upplýsingum er miðlað til, fer með;*

Sömuleiðis væri gott ef þetta endurspeglast í stefnu fyrirtækjanna en þar er oft rætt um að verja eigin innviði en minna rætt um öryggi viðskiptavinanna og umhyggju fyrir kerfum þeirra. Æskilegt er að fyrirtækin líti líka til komandi persónuverndartilskipunar ESB sem að öllum líkindum mun verða innleidd hérlendis árið 2018.

Þess ber að geta að samvinna CERT-ÍS og fyrirtækjanna á skilaði góðum árangri í mörgum málum. Alltaf má þó gera betur og er nauðsynlegt að leggja enn meiri áherslu á umræður, samhæfingu og samstarf í þessum málum á árinu 2016.

Kerfi til upplýsingamiðlunar

Unnið er að endurbótum kerfa sveitarinnar til að miðla og taka á móti upplýsingum og vinna frekar, svo sem móttaka og flokka tilkynningar um atvik, forgangsraða og áframsenda þau til viðkomandi aðila hérlendis, með beiðni um viðbrögð í samræmi við eðli málsins hverju sinni.

Lykiltölur um upplýsingamiðlun

Sveitin vinnur að endurbótum á kerfum og ferlum til að halda utan um atvik og vonast til að geta síðar gefið reglulega út tölfræði vegna atvika.

Stefnumótunarvinna

Eins og nefnt var í síðustu ársskýrslu netöryggissveitarinnar var hópstjóri hennar þátttakandi í vinnuhópi innanríkisráðuneytisins í verkefninu um mótun á netöryggisstefnu Íslands sem lauk um mitt árið. Við tók þátttaka í netöryggisráði þar sem sitja fulltrúar frá opinbera geiranum og hafa það hlutverk að framfylgja aðgerðaráætluninni sem fylgdi stefnunni. Nánari upplýsingar um hlutverk og starf netöryggisráðs er að finna á vef innanríkisráðuneytisins.

Æfingar og þjálfun

Á vettvangi NCC samstarfsins (Nordic CERT Collaboration), tók sveitin, ásamt netöryggissveitum hinna Norðurlandanna, þátt í æfingu í Svíþjóð snemma árs. Tveir starfsmenn fóru héðan, annar tók þátt með sænsku CERT-sveitinni CERT-SE og hinn var í stjórnstöð æfingarinnar. Var þetta hin gagnlegasta æfing og mjög vel að henni staðið. Auk ávinnings af æfingunni sjálfri efldust tengsl við systursveitirnar sem er gríðarlega mikilvægt í starfi sveitarinnar.

Innlend netæfing

Ekki náðist að halda innanlandsæfingu innan þjónustuhóps sveitarinnar á árinu, af ýmsum ástæðum, m.a. vegna þeirrar óvissu sem ríkti um starfsemi sveitarinnar framan af árinu. Netútlaginn var síðast haldinn 2013 og er nauðsynlegt að stefna að slíkri æfingu næsta haust.

Landsþjónusta í hnotskurn

Helstu hlutverk sveitarinnar á landsvísu eru:

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 er CERT sveit til þrautavara, þ.e. þegar aðrar leiðir hafa reynst gagnlausar við að fá lausn mála, svo sem fyrrgreint vefveiðamál. Í þessum tilgangi vísar sveitin 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 sömuleiðis utan um tengiliða- og þjónustuskrá.

Landstengiliðurinn tekur líka þátt í alþjóðlegu samstarfi og átaksverkefnum. Til dæmis er CERT-ÍS þátttakandi í norrænu samstarfi CERT-netöryggissveita eins og fyrr er getið, þar með talið netæfingum. 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 netvá sem hætta er á að breiðist út til netumdæmisins eða gæti snert 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. Má geta þess að fyrsti samráðsvettvangurinn hérlendis var haldinn með þjónustuhópnum undir lok ársins. Hann tókst vel og búast má við góðum afrakstri vinnuhópa sem þar voru ákveðnir og hefja störf á árinu 2016. Unnið verður að framhaldi á slíku samstarfi.

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.

Atvik ársins

CERT-ÍS bárust upplýsingar um nær 800 öryggisatvik hérlendis starfsárið 2015. Þess ber að geta að sumum þessara atvika vísaði sveitin til viðkomandi fyrirtækja hérlendis án sérstakar meðhöndlunar innan hennar og stundum voru fleiri atvik tengd sama málinu. Helstu flokkar mála sem sveitin meðhöndlaði eru eftirfarandi:

Vefveiðar (e. Phishing) og falspóstar

Mikið var um tilkynningar um þjóna sem halda úti falssíðum sem líkja eftir innskráningarsíðum fyrirtækja og hýst eru í íslenskri netlögsögu. Þar getur verið um að ræða þjóna sem settir eru upp sérstaklega til vefveiða en einnig kemur fyrir að um sé að ræða þjóna sem hefur verið spillt, s.s. að gerandinn nýti sér veikleika í vefþjóni eða vefumsjónarkerfi. Í flestum tilfellum var um að ræða árásir gegn erlendum bönkum en einnig kom sveitin að nokkrum málum sem snertu íslensk fyrirtæki. Í flestum tilfellum er notendum beint inn á síður af þessu tagi með vefveiðapóstum (e. Phishing email) og kom CERT-ÍS að meðferð nokkurra slíkra pósta. Í nokkrum mæli varð vart við að íslensk lén væru sett upp til vefveiða og virðist það vera ný þróun frá liðnum árum.

Almennt eru hýsingar og ábyrgðaraðilar fljótir að bregðast við tilmælum um að loka á slíka starfsemi. Þó reyndist í sumum tilfellum snúið að ná til hinna raunverulegu ábyrgðaraðila, þar sem keðja aðila getur á stundum orðið alllöng. Dæmi er um að mismunandi aðilar sjái um hýsingu þjóns, þjóninn sjálfan, sýndarhýsingu fyrir vefsvæði, vefsvæðið sjálft og nafnaþjónustu. Getur þá orðið tímafrekt að ná sambandi við þann aðila sem telur sér heimilt að grípa til aðgerða. Eru í bígerð skýrari verkferlar með löggæslu til að taka fljótt og vel á þessari tegund mála.

Varasamir vefþjónar

Upp komu allnokkur mál þar sem CERT-ÍS rannsakaði þjóna sem telja mátti hættulega netnotendum. Í slíkum tilfellum getur bæði verið um að ræða lögmæta þjóna sem hefur verið spillt sem og þjóna sem sérstaklega eru settir upp í slæmum tilgangi. Algengastar reyndust grunsemdir um að þjónar væru hlekkur í kerfi þjóna sem reyna að setja upp spillikóða á tölvum endanotenda, s.k. "Exploit kit". Slík kerfi senda endanotendum ýmsar tegundir óværu, svo sem "Ransomware", sem dulkóðar skrár notenda og krefst greiðslu fyrir afkóðunarlykil.

Í öllum tilfellum sem CERT-ÍS kom að á árinu tókst farsællega að uppræta slíka þjóna í góðri samvinnu við hýsingaraðila og eigendur þeirra.

Álagsárásir og umferðarmögnun

Allmargar álagsárásir voru gerðar á íslenska upplýsingainnviði á árinu. Einna stærst og mest áberandi var árás sem talin er eiga rætur að rekja til Anonymous samtakanna í nóvember 2015. CERT-ÍS fékk tilkynningar um margar slíkar árásir en kom ekki nema að litlu leyti að meðferð þeirra, þar sem upplýsingainnviðir netþjónustuaðila sjá í flestum tilfellum sjálfvirkt um meðferð þeirra. Mikilvægt er þó að safna upplýsingum um slíkar árásir til að viðhalda ástandsvitund. Einnig kom CERT-ÍS að nokkrum málum þar sem íslenskar IP tölur komu við sögu í árásum gegn erlendum aðilum.

Skannanir og aðrar könnunaraðgerðir

Talsvert var um tilkynningar um skannanir gegn íslenskum og erlendum aðilum. Almennt má segja að slíkar könnunaraðgerðir séu daglegt brauð á netinu og almennt ekki talin ástæða til að meðhöndla eða bregðast við sérstaklega.

Veikleikar og vísbendingar um sýkingar

CERT-ÍS varð áskynja um ýmsa veikleika í upplýsingainnviðum hérlendis sem gætu hafa leitt til sýkingar/spillingar þeirra. Upplýsingar af þessu tagi berast úr fréttaveitum sem sveitin hefur aðgang að sem og úr upplýsingaveitum sem tilkynna ef vísbendingar eru um sýkta þjóna. Sveitin áframsendir slíkar upplýsingar á viðkomandi aðila hérlendis.

APT mál

Sveitinni bárust upplýsingar um örfá s.k. APT (e. Advanced Persistent Threat) mál. Þar er um að ræða alvarlegustu og jafnframt erfiðustu málin í meðferð. Oftast er um að ræða tilfelli þar sem langtíma-takmarkið er að ná fótfestu í upplýsingakerfum stjórnvalda eða hátæknifyrirtækja og afla upplýsinga með leynd. Líkur benda til að þau mál sem rannsökuð hafa verið hér beinist ekki gegn íslenskum aðilum en samkvæmt eðli þeirra er ekki hægt að fjalla frekar um efni þeirra hér.

Á þessu sviði leggur sveitin áherslu á aukna þátttöku í erlendu samstarfi og notkun upplýsingaveitna. Ljóst er að mál af þessu tagi verða alltaf snúin í rannsókn, sérstaklega í þeim tilfellum þar sem um stærri alþjóðlega aðgerð er að ræða sem fara á leynt. Eru í bígerð skýrari verkferlar með löggæslu til að taka fljótt og vel á þessari tegund mála.

Ráðgjöf varðandi önnur mál

CERT-ÍS veitti ráðgjöf í nokkrum öðrum tilfellum sem varða ekki beint kjarnastarfsemina. Má þar nefna fjárkúgunarmál þar sem reynt var að krefjast endurgjalds fyrir upplýsingar sem umræddur aðili taldi sig hafa náð frá íslensku fyrirtæki. Einnig komu upp mál þar sem íslenskir endanotendur höfðu orðið fyrir barðinu á svokölluðum gagnagíslatöku-óværum (e. Ransomware). Þá komu upp mál þar sem vefjum hafði verið spillt og skipt út efni (e. Defacement). Í þessum tilfellum veitti CERT-ÍS ráðgjöf varðandi bestu leiðir til að hreinsa út óværu og koma í veg fyrir spillingu. Almennt eru mál af þessum toga brotastarfsemi sem á heima hjá löggæslu fremur en CERT sveitum.

Erlent samstarf

Norrænt samstarf

Sem fyrr er sveitin virk í NCC samstarfi norrænna CERT netöryggissveita. Nýtist það vel í upplýsingamiðlun milli landanna, en norrænu sveitirnar, svo sem sú í Finnlandi, eru með þeim fremstu á sínu sviði. Til Norðurlandanna er mikla reynslu og þekkingu að sækja og samstarfið því afar mikilvægt.

Samstarf við ENISA

Póst- og fjarskiptastofnun hefur lengi átt gott samstarf við Net- og upplýsingaöryggisstofnun Evrópusambandsins, ENISA, m.a. um CERT málefni, málefni ómissandi upplýsingainnviða og um stefnu ESB í netöryggismálum. Er þessi samvinna eitt af forgangsverkefnum CERT-ÍS, næst á eftir Norðurlandasamstarfinu, enda fæst þaðan sömuleiðis mikil reynsla og þekking á þessu sviði.

Vaxandi ógnir

Ljóst þykir að ógnum gagnvart netöryggi hefur fjölgað á heimsvísu, gerendur orðið þróaðri og ógnirnar því alvarlegri. Netöryggissveitin CERT-ÍS og samstarfsaðilar hennar stefna markvisst að því að auka þekkingu sína á ógnum og efla ástandsvitund hverju sinni. Sveitin leitast við að hafa góða yfirsýn bæði yfir tæknilausnir og aðrar gagnlegar upplýsingar. Miklu máli skiptir að skipulag, þjálfun og heildrænt samstarf í þessum efnum sé ræktað. Sérhvert fyrirtæki og stofnun þarf að vera meðvituð um ábyrgð sína og hlutverk þegar kemur að netöryggi og varðveislu gagna. Ísland sem þjóð þarf að vera undirbúin undir alvarlegar netógnir og viðbrögð við þeim að vera vel samhæfð, undirbúin og þjálfuð.

Enn vantar hérlendis samræmda stefnu, eða leiðbeiningar fyrir íslensk gögn geymd í gagnaskýjum erlendis. Mismunandi lög og reglur gilda um slík gögn eftir því hvar slík ský eru skráð og vistuð. Kemur slíkt líka inn á persónuvernd, því oft innihalda gögnin persónugreinanlegar upplýsingar sem gæta þarf sérstaklega að. Hér þurfa stjórnvöld og einkageirinn að taka höndum saman til að móta heildræna stefnu í þessum og hliðstæðum málum.

Starfsáætlun fyrir 2016

Í starfsáætlun sveitarinnar á árinu 2016 verður meðal annars lögð áhersla á eftirfarandi atriði:

- ✓ Auknar umræður, samráð og samvinna við þjónustuhóp sveitarinnar
- ✓ Settur verði á laggirnar samráðsvettvangur með þjónustuhópi sveitarinnar
- ✓ Stofnaðir verða vinnuhópar innan samráðsvettvangsins sem gera m.a. eftirfarandi:
  - o „Viðbragðsáætlun þjónustuhóps CERT-ÍS gegn netvá
  - o Undirbúa og halda innanlands-netæfingu 2016 fyrir áramótin 2016/2017,
  - o Leiðbeiningar um tilkynningar til sveitarinnar
- ✓ Meiri samvinna með markaðaaðilum um lausn ýmissa mála, s.s. vefveiða (e. Phishing)
- ✓ Samskipti við framkvæmdavaldið verði efld

- ✓ Fylgst verði með þróun regluverks um netöryggi innan ESB og vakin athygli á henni hérlendis