Samningur milli fjármála- og efnahagsráðuneytis og Póst- og fjarskiptastofnunar um GovCERT-þjónustu Netöryggissveitarinnar (CERT-ÍS)

1. Markmið og gildissvið

Markmið þjónustusamnings þessa er að treysta getu samfélagsins, þar á meðal þjónustukaupa til að verjast öryggisatvikum, svo sem netárásum, njósnum (t.d. APT atlögum) og öðrum alvarlegum atvikum þar á meðal í þeim tilgangi að greina og gefa viðvörun þegar um alvarlegar samhæfðar árásir gegn ómissandi upplýsingainnviðum þjónustukaupa er að ræða. Með samningi þessum tekur þjónustusali að sér að veita þjónustukaupa netöryggisþjónustu, sérsniðna að þörfum hins opinbera (svonefnda GovCERT þjónustu). Á samningstímanum skal áhersla lögð á þjónustu við ráðuneyti Stjórnarráðs Íslands.

Um er að ræða þjónustusamning milli þjónustusala og þjónustukaupa sem ætlað er að þróa og efla þjónustu þjónustusala við þjónustukaupa og um leið aðlaga þjónustuna að því fyrirkomulagi sem að er stefnt í kjölfar innleiðingar hinnar svokölluðu NIS-tilskipunar (EU 2016/148 varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum innan Evrópusambandsins).

2. Aðild

Aðilar að samningi þessum eru netöryggissveit Póst- og fjarskiptastofnunar, CERT-ÍS, kt. 570397-2499, hér eftir nefndur þjónustusali og fjármála- og efnahagsráðuneytið, kt. 550169-2829, hér eftir nefndur þjónustukaupi, vegna GovCERT þjónustu fyrir stjórnsýsluna (A-hluta ríkissjóðs).

Samningsaðilar geta veitt öðrum ríkisstofnunum heimild til þess að gerast viðbótaraðilar að samningi þessum og njóta þær þá réttinda og gegna skyldum sem þjónustukaupi í skilningi hans. Um viðbótaraðild ríkisstofnunar skal getið í sérstökum viðauka við samning þennan. Sé ekki um annað samið við viðbótaraðila gilda öll ákvæði samnings þessa sem og viðaukum við hann að því undanskildu að sérstaklega skal samið um fjárhæð þjónustugjalds, sbr. 7. gr. samnings þessa, sem þjónustusali innheimtir af hlutaðeigandi stofnun. Þjónustugjaldið skal taka mið af því umfangi sem felst í þjónustu við stofnunina.

3. Lagaheimildir og forsendur samnings

Samningurinn er gerður á grundvelli laga um starfsemi netöryggissveitar Póst- og fjarskiptastofnunar. Við undirritun eru það lög um fjarskipti nr. 81/2003, og þá sérstaklega grein 47 a, Öryggis- og viðbragðshópur til verndar ómissandi upplýsingainnviðum, auk reglugerðar nr. 475/2013 um málefni CERT-ÍS netöryggissveitar, sérstaklega 14. greinar um þjónustusamninga, sjá nánar í viðauka I.

4. Almennar skyldur þjónustusala við alla þjónustukaupa

Þjónustusali samræmir viðbrögð innan alls samfélagsins þegar um alvarleg atvik er að ræða sem snerta net- og upplýsingaöryggi mikilvægra innviða samfélagsins, en áhersla í þjónustu er við þjónustukaupa. Þjónustusala er ætlað að sinna ráðgjöf, vara við og veita aðstoð við netöryggistengd atvik, svo sem greiningar og þróun ástandsmyndar.

Þjónustusali er landstengiliður vegna netöryggis. Sem slíkur kemur þjónustusali fram fyrir hönd Íslands á alþjóðavettvangi, tekur þátt í samstarfsverkefnum, þar á meðal æfingum og tekur á móti öryggisflokkuðum upplýsingum um netvá frá landstengiliðum annarra landa, sem og tilkynningum um öryggisatvik.

Markhópur þjónustusala eru rekstraraðilar ómissandi upplýsingainnviða samfélagsins, hvort sem um einka- eða opinbera aðila er að ræða og sem gert hafa samning við þjónustusala. Þjónustusali vinnur með öðrum aðilum að þessu markmiði, þar á meðal embætti ríkislögreglustjóra, erlendum netöryggissveitum, erlendum samstarfsstofnunum og einkaaðilum. Þjónustugjöldum rekstraraðila er ætlað að standa undir tilsvarandi hluta á rekstri þjónustusala.

Þjónustusali kemur fram fyrir hönd stjórnvalda gagnvart almenningi varðandi þá þætti er snúa að þjónustu hans, t.d. með upplýsingamiðlun um aðsteðjandi netvá eða yfirstandandi netárás.

Þjónustusali skal eftir fremsta megni veita þá aðstoð sem tilgreind er í viðauka III við samning þennan og aðstoða aðila við að glíma við atvik sem snerta net- og upplýsingaöryggi samkvæmt ákvæðum samnings.

Þjónustusali skal tilkynna þjónustukaupa ef þjónustusali grípur að eigin frumkvæði til einhverra varnaraðgerða.

Þegar um umfangsmikinn atburð (árás) er að ræða getur þjónustusali þurft að forgangsraða þjónustu sinni til að lágmarka samfélagslegan skaða og skal þá miða við eftirfarandi forgangsröðun:

1. Þjóðaröryggi.
2. Öryggi mikilvægra samfélagslegra innviða.
3. Alvarleg atvik er snerta í heild einn geira rekstraraðila mikilvægra samfélagslegra innviða.
4. Atvik er snerta rekstraraðila sem eiga aðild að þessum samningi.
5. Önnur atvik.

Þjónustusali safnar og samræmir upplýsingar sem honum berast um málefni þjónustukaupa og þess geira samfélagsins sem hann tilheyrir. Þjónustusali nýtir upplýsingar um aðsteðjandi ógnir til að móta ógnarmynd fyrir viðkomandi geira sem deilt er reglulega, og þegar tilefni er til, með sérstökum tilkynningum. Ógnarmynd er trúnaðarmál milli þjónustusala og þjónustukaupa að uppfylltum skilyrðum upplýsingalaga nr. 140/2012.

Þjónustusali veitir þjónustukaupa, eftir föngum, ráðgjöf varðandi tilhögun/virkni netvarna sinna en ábyrgð á netvörnum er þó ávallt þjónustukaupa, sbr. kafla 4.

5. Ábyrgð þjónustukaupa

1. Þjónustukaupi ber ábyrgð á eigin net- og upplýsingaöryggi. Í því felst m.a. að þjónustukaupi ber ábyrgð á því að koma á skipulagi sem miðar að því að tryggja rekstraröryggi upplýsingakerfa sinna. Þjónustusali veitir eftir föngum ráðgjöf varðandi öryggishögun, sbr. kafla 4.
2. Taka skal mið af ábendingum þjónustusala eftir því sem við á við útfærslu á upplýsingaöryggi þjónustukaupa.
3. Þjónustukaupi skal tilkynna þjónustusala um alvarlegar ógnir og atvik sem steðja að kerfum þjónustukaupa, einkum þegar um er að ræða ógnir sem geta steðjað að viðkomandi geira í hluta eða í heild. Slíkar upplýsingar eru veittar í trúnaði að uppfylltum skilyrðum upplýsingalaga nr. 140/2012. Jafnframt gilda um upplýsingarnar þær reglur sem skilgreindar eru í viðauka IV. Ef slíkar upplýsingar innihalda persónupplýsingar skal miðlun þeirra vera í samræmi við lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga.
4. Aðili ber ábyrgð á að við framkvæmd ákvæða þessa samnings sé jafnframt tryggt að kröfur laga og reglugerða um aðra þætti rekstursins séu uppfylltar, t.d. varðandi persónuvernd og samkeppni.

6. Samskipti og trúnaður

Þjónustukaupi tilnefnir tvo tengiliði sem sinna yfirstjórn hjá þjónustukaupa. Einnig tilnefnir þjónustukaupi tvo tæknilega tengiliði sem sinna daglegum samskiptum við þjónustusala hvað varðar meðhöndlun öryggisatvika og upplýsingaskipti.

Almennt skal ríkja þagnarskylda og trúnaður um upplýsingar sem fara á milli þjónustusala og þjónustukaupa, sjá nánar í viðauka IV.

7. Þjónustugjald

Starfsemi þjónustusala er fjármögnuð með þjónustugjöldum sem taka mið af þörfum og þjónustu sem sérhverjum aðila að samningi þessum er veitt. Semja skal sérstaklega um hvernig greiðslu skuli háttað vegna ósamningsbundinna verkefna sem upp kunna að koma og óskað er eftir að þjónustusali sinni.

Framlag þjónustukaupa vegna samnings þessa er kr. 30.000.000.- og er það bæði til að mæta stofn- og rekstrarkostnaði, hugsanlega vegna ráðningar á nýjum starfsmanni. Við undirritun samnings þessa greiðir þjónustukaupi þjónustusala kr. 15.000.000.- og það sem eftir stendur framlagsins greiðast þjónustusala þegar umræddur starfsmaður hefur störf eða við annan áfanga sem bæði þjónustukaupi og þjónustusali koma sér saman um að miða skuli við.

8. Vanefndir, úrræði gegn vanefndum og meðferð ágreiningsmála

Telji þjónustukaupi vanefndir á samningi þessum eða framkvæmd verks ábótavant, þrátt fyrir frest til úrbóta, skal gerð skrifleg athugasemd þar að lútandi. Hið sama gildir telji þjónustusali vanefndir vera á samningi þessum.

Ef ágreiningur verður milli aðila um gildi, túlkun eða framkvæmd samningsins skulu þeir leitast við að semja um lausn vandans sín á milli.

Náist ekki samkomulag um úrbætur skulu mál sem kunna að rísa vegna brota á samningi þessum eða vegna ágreinings um túlkun hans rekin fyrir Héraðsdómi Reykjavíkur eða fyrir *ad hoc* gerðardómi ef aðilar sammælast um það.

9. Innleiðing þjónustu

Aðilar samningsins semja um það sín á milli hvernig staðið skal að innleiðingu þjónustunnar. Sjá nánar í viðauka III.

10. Gildistími og lok samnings

Samningur þessi gildir til 1. janúar 2019 þegar áætlað er að nýtt fyrirkomulag netöryggis, byggt á NIS-tilskipuninni, tekur gildi. Dragist innleiðing tilskipunarinnar fram yfir lokadagsetningu samnings þessa skulu samningsaðilar leitast við að tryggja framhald á þjónustunni með nýjum samningi, allt þar til skipulag byggt á NIS-tilskipuninni hefur tekið gildi. Samningsaðilar eru sammála um að ákvæði samnings þessa og viðaukar við hann endurspegli að um þróunartímabil er að ræða, þ.m.t. ákvæði um umsamda þjónustu og þjónustugjald. Samningurinn hefur því ekki fordæmisgildi hvað snertir það fyrirkomulag sem stefnt er að með innleiðingu NIS tilskipunarinnar.

Stefnt skal að því að fara yfir stöðu samnings þessa á tveimur samráðsfundum á samningstímanum þar sem m.a. verður farið yfir stefnumótun og sett mælanleg markmið þar sem við á.

Reykjavík, 25. janúar 2018

f.h. fjármála- og efnahagsráðuneytis

_____

Sverrir Jónsson, skrifstofustjóri

f.h. Póst- og fjarskiptastofnunar

_____

Hrafnkell V. Gíslason, forstjóri

Eftirtaldir viðaukar eru hluti samnings þessa

- **I. Hlutverk þjónustusala skv. lögum**
- **II. Hlutverk þjónustukaupa**
- **III. Sérákvæði um þjónustu þjónustusala við þjónustukaupa**
- **IV. Samskipti og trúnaður**

Viðaukar við þjónustusamning CERT-ÍS

Viðauki I - Hlutverk þjónustusala skv. lögum

Samningurinn er gerður á grundvelli laga um starfsemi netöryggissveitar Póst- og fjarskiptastofnunar. Við undirritun eru það lög um fjarskipti nr. 81/2003, og þá sérstaklega grein 47 a, *Öryggis- og viðbragðshópur til verndar ómissandi upplýsingainnviðum*, auk reglugerðar nr. 475/2013 um málefni CERT-ÍS netöryggissveitar, sérstaklega 14. greinar um þjónustusamninga.

Í lögum um fjarskipti nr. 81/2003 segir í grein 47 a um hlutverk netöryggissveitar PFS:

> Netöryggissveitin skal gegna hlutverki CERT-teymis fyrir Ísland og skal hún taka þátt í og gegna hlutverki tengiliðar íslenskra stjórnvalda í innlendu og alþjóðlegu samstarfi um viðbragðsvarnir vegna net- og upplýsingaöryggis. Markmiðið með starfsemi netöryggissveitarinnar er að fyrirbyggja og draga úr hættu á netárásum og öðrum öryggisatvikum á netumdæmi eins og kostur er og sporna við og lágmarka tjón á ómissandi upplýsingainnviðum sem af slíku kann að hljótast.
>
> Netöryggissveitin skal leitast við að greina öryggisatvik á frumstigi og fyrirbyggja að þau breiðist út og valdi tjóni á ómissandi upplýsingainnviðum sem falla undir netumdæmi hópsins. Skal netöryggissveitin aðstoða þjónustuhópinn við forvarnir, leiðbeina honum og styðja við skjót viðbrögð gegn aðsteðjandi hættu. Við útbreitt öryggisatvik samhæfir netöryggissveitin aðgerðir aðila þjónustuhópsins gegn aðsteðjandi hættu til að lágmarka tjón og reisa við óvirk kerfi. Netöryggissveitin veitir þjónustuhópnum ráðgjöf um varnir og viðbúnað og kemur upplýsingum á framfæri við almenning ef þurfa þykir.

Þá er hlutverk CERT-ÍS skilgreint í reglugerð nr. 475/2013, 4. gr., með eftirfarandi hætti:

> Netöryggissveitinni er ætlað að fyrirbyggja, draga úr og bregðast við hættu vegna netárása eða hliðstæðra öryggisatvika eins og kostur er í þeim tölvukerfum sem falla innan netumdæmis hennar. Þetta gerir sveitin m.a. með því að stuðla að efldum forvörnum og viðbragðsstarfsemi, í samvinnu og samstarfi við þjónustuhóp sinn. Helsta hlutverk sveitarinnar er að styðja þjónustuhópinn við að takast á við ógnir og öryggisatvik. Sveitin leitast við að greina öryggisatvik sem ógna heildstæði og öryggi ómissandi upplýsingainnviða, takmarka útbreiðslu atvikanna og tjón af þeirra völdum. Við útbreidd og alvarleg öryggisatvik skal sveitin samhæfa viðbrögð og aðgerðir innan netumdæmisins.

Netöryggissveitin gegnir hlutverki landstengiliðs (e. National Point of Contact) vegna netöryggisatvika innan íslenskrar netlögsögu.

Hlutverk þjónustusala vegna fyrirhugaðrar innleiðingar NIS tilskipunarinnar

Gera má ráð fyrir að þjónustusala verði falið það hlutverk að vera samræmingaraðili viðbragðsvarna vegna net- og upplýsingaöryggis þeirra innviða sem munu heyra undir NIS tilskipunina (e. The Directive on security of network and information systems). NIS tilskipunin kveður m.a. á um skyldur rekstraraðila mikilvægra innviða varðandi eftirfarandi:

- Rekstraraðilar grípi til viðeigandi og hæfilegra tæknilegra og skipulagslegra ráðstafana til að takast á við þá áhættu sem beinist að öryggi net- og upplýsingakerfa sem þeir nota í starfsemi sinni.
- Þessar ráðstafanir skulu tryggja öryggisstig net- og upplýsingakerfa í samræmi við metna áhættu og nýjustu tækni.
- Rekstraraðilar grípi til viðeigandi aðgerða til að fyrirbyggja og lágmarka tjón sem hlýst af atvikum tengdum öryggi net- og upplýsingakerfa með það að markmiði að tryggja samfellu í rekstri slíkra kerfa.
- Rekstraraðilum ber skylda til að tilkynna um öryggisatvik eins fljótt og auðið er.

Hlutverk sveitarinnar er fyrst og fremst stuðningur við þjónustukaupa. Það lýtur ekki að því að framkvæma aðgerðir þjónustukaupa gegn öryggisatvikum. Þjónustusali aðstoðar við greiningu á orsökum þeirra (glæpsamleg, þrýstihópar, ríki eða aðilar beint eða óbeint á þeirra vegum). Aðkomu lögreglu þarf hugsanlega við þessa greiningu og við það að hafa upp á gerendum og hugsanlegum refsingum ef slíkt á við.

Viðauki II – Hlutverk þjónustukaupa

Hlutverk þjónustukaupa er samstarf við þjónustusala þar sem áhersla er lögð á uppbyggingu og þróun viðbragðsstarfsemi, sem og fyrirbyggjandi aðgerðir til að sporna við stærri og smærri öryggisatvikum og ógnum sem valdið geta netvá. Í þessu samhengi bregst þjónustukaupi við tilmælum þjónustusala um heildrænt samstarf, aðgerðir, skipulag, viðbragð og uppbyggingu til lengri eða skemmri tíma. Sama gildir um mótun og endurbætur ýmissa gæðaskjala þjónustukaupa, eins og áherslu í stefnu viðkomandi, um verklagsreglur, vinnuleiðbeiningar, ferla við upplýsingaskipti og samskipti. Enn fremur sýnir þjónustukaupi eða eftir atvikum afhendir umbeðin afleidd gæðagögn til að mynda niðurstöðu áhættumats, innihald dagbókakerfa eða skjölun og samskiptasögu í tilteknum máli.

Miðað er við að aðili hafi formgert umhverfi upplýsingaöryggis hjá sér með viðeigandi hætti, til dæmis með því að miða við ISO 27001 staðal hvað varðar þá hluta rekstrar síns sem snúa að öryggi kerfa og fá eftir atvikum vottun þar að lútandi.

Í samræmi við ákvæði NIS tilskipunarinnar tilkynnir þjónustukaupi sveitinni um öryggisatvik sem upp koma, eða geta komið í eigin kerfum. Þjónustusali skilgreinir viðmið um þessar tilkynningar að höfðu samráði við þjónustukaupa.

Viðauki III - Sérákvæði um þjónustu þjónustusala við þjónustukaupa

Markmiðið með starfsemi þjónustusala er að fyrirbyggja og draga úr hættu á netárásum og öðrum öryggisatvikum í netumdæmi þjónustusala eins og kostur er og sporna við og lágmarka tjón á ómissandi upplýsingainnviðum sem af slíku kann að hljótast.

Hér á eftir eru taldir upp þeir flokkar verkefna sem þjónustusali sinnir og falla undir samning þennan. Um er að ræða breitt svið verkefna og því er nauðsynlegt að forgangsraða. Þjónustusali mun í upphafi hvers starfsárs útbúa starfsáætlun sem kynnt verður fyrir aðilum samnings sem trúnaðarmál og þar sem tiltekin eru helstu verkefni og umfang þeirra. Verkefnum verður raðað í forgangsröð og reglulega kynnt skýrsla um framvindu þeirra á samráðsfundum. Telji samningsaðilar að þörf sé á auknu umfangi verður samið um slík verkefni sérstaklega og miðað við að endurskoða þennan samning að ári liðnu til að endurspegla aukið umfang. Þjónustusali áskilur sér rétt til að forgangsraða verkefnum eftir stöðu mála hjá einstökum aðilum og netlögsögunnar í heild. Þannig er viðbragð við öryggisatvikum ávallt í forgangi umfram hvers kyns undirbúningsverkefni.

Skyldur þjónustusala við þjónustukaupa

1. Veita aðila stuðning um viðbrögð við netvá, sjá þó ákvæði um forgangsröðun.
2. Sjá um samhæfingu aðgerða innan þjónustuhópsins gegn netvá.
3. Aðvara aðila ef óeðlileg umferð gagna tengdum hópnum greinist eða aðrar vísbendingar eru um öryggisatvik sem geta haft áhrif á þeirra kerfi.
4. Deila viðeigandi upplýsingum til aðila frá alþjóðlegu tengslaneti sínu.
5. Veita aðila aðstoð við greiningar á almennum atvikum, sjá þó ákvæði um forgangsröðun viðbragða.
6. Veita ráð og upplýsingar til að aðstoða aðila við að koma starfsemi sinni í eðlilegt horf eftir atvik.
7. Koma á samráðsvettvangi á milli samningsbundinna aðila innan viðkomandi geira þar sem unnt verði að skiptast á tæknilegum öryggisupplýsingum til varnar gegn netvá og til að samhæfa aðgerðir gegn alvarlegum atvikum og afleiðingum þeirra.
8. Bjóða stjórnendum samningsaðila til samráðsfundar að minnsta kosti tvisvar á ári. *(einnig varðandi stöðu samstarfs).*
9. Upplýsa aðila um aðra viðburði sem geta stuðlað að bættum upplýsingaskiptum.
10. Veita leiðsögn til að koma upp dulritunarvarinni samskiptaleið á milli sveitarinnar og aðila, sjá viðauka IV.
11. Halda reglulegar æfingar þar sem viðbrögð við netöryggisatvikum verða æfð, aðstoð við skipulag æfinga sem þjónustukaupar kunna að standa fyrir og að taka þátt í innlendum og erlendum æfingum samkvæmt nánara samkomulagi við þjónustukaupa eða fyrir þeirra hönd.

Samráð og fræðsla

Þjónustusali rekur samráðsvettvang fyrir aðila þessa samnings. Fundir eru að jafnaði boðaðir á tveggja mánaða fresti eða oftar ef þörf er á. Boðað verður til sérstakra samráðsfunda án tafar í tilvikum þar sem metið er svo að bráð hætta stafi að einstökum geirum. Markmið funda er að:

- Skiptast á upplýsingum við þjónustusala um stöðu aðila samnings og þeirra áherslur í öryggismálum.
- Fjalla um forgangsröðun þjónustusala varðandi dagleg verkefni, átaksverkefni og meðhöndlun atvika.
- Ráðleggja aðilum þjónustuhópsins um öryggismál, miðla upplýsingum um aðsteðjandi ógnir og aðferðir til að verjast þeim.
- Miðla samræmdum upplýsingum um atvik sem átt hafa sér stað hjá aðilum samnings, innan þeirra marka sem trúnaður við einstaka aðila leyfir.
- Efla tengsl við aðra viðbragðsaðila, s.s. löggæslu (nánar er kveðið á um í samningi hverjir taka þátt í fundum en þar getur m.a. verið um að ræða fulltrúa RLS og LRH).
- Vera vettvangur fyrir upplýsingaskipti í trúnaði milli aðila (TLP:Rautt, samkvæmt trúnaðarflokkun sem lýst er í viðauka IV).
- Fjalla um áherslur í fræðslu og leggja línur um forgangsröðun verkefna í uppbyggingu öryggismála.

Viðbragðsþjónusta (meðhöndlun öryggisatvika)

Þjónustusali byggir upp tengslanet aðila í þjónustu og er gert ráð fyrir að jafnaði tveimur frá hverjum aðila sem samningurinn nær til. Tengiliðagrunni er haldið við af CERT-IS og hann nýttur þegar öryggisatvik eiga sér stað (sjá nánari skilgreiningu á hvað telst vera öryggisatvik). Viðbragð þjónustusala við öryggisatvikum fer eftir umfangi atviks og nauðsynlegri forgangsröðun hverju sinni en getur falist í:

- Miðlægri upplýsingasöfnun þar sem aðilar samnings upplýsa þjónustusala um stöðu mála og málsatvik eru skráð í upplýsingakerfi sveitarinnar.
- Öflun nánari upplýsinga um atvik, s.s. árásaraðila og verkfæri, frá upplýsingaveitum, þ. á m. erlendum CERT sveitum.
- Samræming á aðgerðum s.s. samræmd ástandsvitund, miðlun upplýsinga og ráðgjöf við einstaka aðila samnings og til hópsins í heild.
- Greining gagna, s.s. færsluskráa (logga) og spillikóða (hér getur verið um að ræða þjónustu sem þarf að kaupa af innlendum sem erlendum aðilum).
- Ráðgjöf um aðgerðir til einstakra aðila samnings eða hópsins í heild eftir atvikum.
- Ráðgjöf, upplýsingaöflun og viðbragð í starfsstöð samningsaðila.

Þjónustusali rekur stjórnstöð fyrir öryggisatvik á Vínlandsleið 2-4 í Reykjavík og er hún mönnuð á dagvinnutíma. Þó leitast þjónustusali eftir föngum við að manna stjórnstöð innan 8 tíma í neyðartilvikum. Stjórnstöð er með trygg sambönd við aðra viðbragðsaðila, þ. á m. gegnum Tetra kerfi og upplýsingakerfi sem notuð eru til að stjórna atvikum og skapa ástandsvitund. Viðbragðsþjónustu þjónustusala er nánar lýst á vefnum www.cert.is. Þjónustusali hefur umsjón með skráningum aðila að samningnum í boðunargrunninn *Bjargir* og sér um reglubundnar prófanir á samskiptum í gegnum það kerfi.

Þjónustusali skipuleggur og tekur þátt í neyðarstjórn sem skipuð er helstu aðilum samnings samkvæmt viðbragðsáætlun þjónustusala og þjónustuhópsins. Neyðarstjórn er boðuð þegar stærri atvik eiga sér stað sem talin eru ógna samningsaðilum í heild eða öryggi mikilvægra upplýsingainnviða landsins. Reglulegir fundir eru haldnir með neyðarstjórn, a.m.k. tvisvar á ári og hún er upplýst um stöðu mála hverju sinni. Einnig tekur neyðarstjórn þátt í reglubundnum æfingum. Hlutverki neyðarstjórnar er nánar lýst í viðbragðsáætlun.

Vöktun og ástandsvitund

Þjónustusali rekur kerfi sem vakta ýmsar upplýsingaveitur sem geta gefið vísbendingar um stöðu íslensku netlögsögunnar. Þar má m.a. telja erlendar upplýsingaveitur sem reka ákveðnar netgildrur (e. honeypots) og veiða umferð svokallaðra yrkjanetsþjóna (e. botnet servers) og skönnunarþjónustur sem birta reglulega upplýsingar um veikleika í einstökum kerfum. Einnig tekur þjónustusali sem landstengiliður við kvörtunum og ábendingum aðila um misnotkun (e. abuse) kerfa, safnar í upplýsingabanka og kemur skilaboðum til aðila sem geta brugðist við eftir atvikum. Þjónustusali fylgist einnig með fréttum um uppgötvaða veikleika og safnar í upplýsingabanka.

- Þjónustusali miðlar upplýsingum um birta veikleika til aðila samnings. Til að bæta þá þjónustu geta aðilar upplýst þjónustusala um þau kerfi í sínum rekstri sem talin eru mikilvægust.
  Þjónustusali miðlar einnig upplýsingum um kerfi í rekstri aðila samnings sem eru veik fyrir samkvæmt upplýsingaveitum þjónustusala til einstakra ábyrgðaraðila viðkomandi kerfa. Þjónustusali veitir ráðgjöf um viðbrögð og forgangsröðun vegna uppgötvaðra veikleika. Tölfræðiskýrsla um almennt ástand netlögsögunnar sem snýr að þjónustukaupa verður afhent mánaðarlega.
- Þjónustusali (í hlutverki sínu sem landstengiliður) kemur upplýsingum um misnotkun (e. abuse) til skila til ábyrgðaraðila kerfa og beitir sér eftir föngum við úrlausn slíkra mála, hvort sem um aðila samnings er að ræða eða ekki. Með þessum hætti stuðlar þjónustusali að betri stöðu netlögsögunnar sem nýtist jafnt aðilum samnings sem öðrum íslenskum aðilum.

Þjónustusali getur boðið upp á vöktunarþjónustu með kerfum einstakra aðila samnings samkvæmt nánari skilgreiningu. Í stuttu máli felur sú þjónusta í sér að settar verði upp safnstöðvar (sýndarvélar eða vélbúnaður) á kerfum samningsaðila sem sendir upplýsingar með öruggum hætti til kerfis í stjórnstöð þjónustusala sem nýttar verða til að vakta vísbendingar um öryggisatvik í einstökum kerfum. Samningar við hvern og einn aðila verða gerðir um slíka vöktun þar sem kveðið verður á um umfang upplýsingaöflunar, trúnað og verð.

Þjónustusali rekur ákveðnar tegundir kjarnaþjónustu til að geta gegnt sínu hlutverki við vernd mikilvægra upplýsingainnviða sem koma til með að nýtast öllum þjónustuhópum sveitarinnar. Hér er um að ræða vélbúnað og stýrikerfi upplýsingakerfis og þjóna, s.s. gagnagrunnsþjóna og vefþjóna. Einnig getur verið um að ræða keypta þjónustu, s.s. aðgang að upplýsingaveitum og rannsóknahugbúnaði. Gert er ráð fyrir að umræddar tegundir þjónustu

nýtist sem best við þjónustu sem snýr að öllum þjónustuhópum sveitarinnar. Reglulega verður gerð grein fyrir kjarnategundum þjónustu í rekstri og kostnaði sem þeim tengist á samningstímanum. Einnig verður áætlun um innkaup og aðrar breytingar á þjónustu borin upp á samráðsfundum. Kostnaður við tegundir þjónustu sem þessa dreifist jafnt milli þjónustuhópanna.

Þjónustusali gerir reglulega skýrslu um almenna þróun og stöðu öryggisatvika og hættu af þeirra völdum. Skýrslunni er dreift meðal þjónustuhópsins. Loks stuðlar sveitin að gerð verði ástandsmynd þegar tiltekið ástand ríkir af völdum netvár, skv. viðbragðsáætlun sveitarinnar og þjónustuhóps hennar. Þessum gögnum er miðlað til samstarfsaðila eftir því sem þörf krefur.

Þjónustusali tekur þátt í samstarfi erlendra CERT sveita og er m.a. fullgildur þátttakandi í NCC samstarfi norrænu CERT sveitanna. Í tengslum við samstarfið rekur þjónustusali útstöð sem tengist öryggisvottuðu upplýsingaskiptaneti NCC. Þjónustusali nýtir upplýsingar sem berast um kerfið til að skiptast á trúnaðarflokkuðum upplýsingum við norrænu sveitirnar. Sveitin miðlar gögnum úr kerfinu eða afleiddum upplýsingum úr því ef þurfa þykir og íslensk lög og trúnaðarmerkingar gagnanna veita heimild til. Slíkar upplýsingar geta nýst samningsaðilum þegar fyrrgreind skilyrði eru uppfyllt.

Þjálfun og æfingar

Þjónustusali veitir ráðgjöf og fræðslu um öryggismál til starfsfólks aðila samnings og tengiliða sinna. Umfang verkefna, tímasetning þeirra og efnistök er nánar ákveðin á samráðsfundum. Sé um að ræða verkefni sem eru utan þess sem telja má innan samnings verður samið um hvert og eitt sérstaklega.

Þjónustusali miðlar upplýsingum til tengiliða sinna um viðbragð við öryggisatvikum, þ. á m. tilkynningar um atvik og örugg samskipti. Eru þessi gögn hugsuð til uppbyggingar á gæðakerfum aðila og samræmingar viðbragða. Samráðsfundir eru m.a. haldnir í þeim tilgangi að skilgreina gæðaskjöl og átaksverkefni. Um einstök verkefni geta verið stofnaðir vinnuhópar aðila sem þjónustusali leiðir.

Þjónustusali stendur fyrir reglubundnum æfingum sem miða að því að samræma viðbrögð allra aðila. Miðað er við stóra æfingu með aðkomu sem flestra aðila á tveggja ára fresti. Æfingar eru skipulagðar á samráðsvettvangi þjónustuhópsins og er miðað við að stofnað sé til vinnuhóps aðila sem sér um skipulagningu um hverja æfingu, framkvæmd, sem og mat og skýrslugerð að æfingu lokinni. Einnig verða haldnar smærri æfingar eftir því sem,tilefni er til, s.s. til að prófa samskiptakerfi og boðleiðir.

Þjónustusali getur einnig tekið þátt í erlendum æfingum að eigin frumkvæði eða frumkvæði verkkaupa og að höfðu samráði við hann með svipuð markmið og að ofan greinir, auk þess að efla boðskipti og samstarf við útlenda samstarfsaðila.

Innleiðing þjónustu - áfangar

Eftirfarandi áfangar verða við innleiðingu:

1. Greining á þörfum og óskum þjónustuhópsins um sérfræðiþekkingu og fyrirkomulag mönnunar.
2. Ráðning eða flutningur starfsmanns/a í netöryggissveitina.
3. Upphafsþjálfun starfsmanns/samstarfsmanna netöryggissveitarinnar /starfsmanna þjónustukaupa ásamt uppsetningu umsaminna kerfa og þjálfun í notkun þeirra ef við á.
4. Upphaf formlegrar þjónustu.

Viðauki IV – Samskipti og trúnaður

Ríkja skal þagnarskylda og trúnaður um allar upplýsingar sem Netöryggissveit fær frá þjónustukaupa nema um opinberar upplýsingar sé að ræða eða upplýsingar ætlaðar til opinberrar birtingar.

Þjónustusali er bundinn trúnaði varðandi allar upplýsingar sem hann kann að verða áskynja í starfi sínu fyrir þjónustukaupa, óháð því hvort viðkomandi upplýsingar teljast til starfsemi sem tengist þessum samningi. Aðilar samnings nota TLP-trúnaðarflokkun við deilingu upplýsinga sín á milli eins og nánar er lýst hér á eftir. Við meðferð atviks kann að reynast nauðsynlegt að miðla upplýsingum sem varða nauðsynleg viðbrögð víðar en upphafleg trúnaðarflokkun þeirra heimila, s.s. til aðila þjónustuhóps, annarra þjónustuhópa rekstraraðila mikilvægra upplýsingainnviða eða viðbragðsaðila. Í slíkum tilvikum munu báðir aðilar samnings ávallt leita heimildar þess sem veitti viðkomandi upplýsingar til að víkka trúnaðarskilgreininguna eins og nauðsynlegt þykir.

Netöryggissveit er skylt að upplýsa ríkislögreglustjóra um netöryggisatvik sem hafa áhrif á rekstrarhæfi eins eða fleiri mikilvægra upplýsingainnviða. Einnig er þjónustusala heimilt, að höfðu samráði við rekstraraðila þeirra ómissandi upplýsingainnviða sem í hlut eiga, að tilkynna ríkislögreglustjóra um meint brot sem talin eru ógna eða hafa ógnað öryggi viðkomandi innviða. Kveðið er á um upplýsingagjöf til ríkislögreglustjóra í reglugerð 475/2013, 11. gr.

Öll meðferð upplýsinga varðandi þennan samning skal vera í samræmi við lög nr. 77/2000 um persónuvernd og lög um meðferð persónuupplýsinga og upplýsingalög nr. 140/2012.

Um upplýsingamiðlun milli aðila gildir eftirfarandi:

- Um meðferð trúnaðarflokkaðra upplýsinga á stiginu TAKMARKAÐUR AÐGANGUR, TRÚNAÐARMÁL, LEYNDARMÁL og ALGJÖRT LEYNDARMÁL gilda ákvæði Reglugerðar 959/2012.
- Aðrar upplýsingar eru meðhöndlaðar samkvæmt TLP (e. *Traffic Light Protocol*) flokkun og er miðað við IS-TLP eins og skilgreint í https://www.trusted-introducer.org/ISTLPv11.pdf. Aðilar þessa samnings skuldbinda sig til að virða TLP merkingar gagna sem þeim berast.
- Miða skal við að upplýsingar séu sendar á milli Netöryggissveitar og aðila í PGP dulritunarvörðum tölvupósti eða annarri tryggri aðferð sem Netöryggissveitin samþykkir. Notast má við póstforrit sem dulkóða tölvupóst í heild eða senda dulritað skjöl sem viðhengi í samskiptum við þjónustusala þar sem trúnaðar er krafist. Opinberan PGP lykil CERT-IS er að finna á heimasíðu sveitarinnar (https://www.cert.is). Meðferð og viðhald dulritunarlykla aðila þessa samnings er á ábyrgð hvers og eins en þjónustusali leitast við að leiðbeina um bestu aðferðir við slíkt.