Nr. 475 26. apríl 2013

REGLUGERÐ

um málefni CERT-ÍS netöryggissveitar.

I. KAFLI

Gildissvið, lögsaga og skilgreiningar.

1. gr.

Gildissvið og markmið.

Reglugerð þessi gildir um starfsemi CERT-ÍS netöryggissveitar Póst- og fjarskiptastofnunar (nefnd netöryggissveit eða sveit) sem og þjónustuhóp sveitarinnar. Ákvæði reglugerðarinnar taka jafnframt til samstarfs og upplýsingaskipta við ytri aðila sem sveitin hefur samskipti við vegna verkefna sinna.

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

2. gr.

Skilgreiningar.

Merking einstakra hugtaka í reglugerðinni er sem hér segir:

1. *Íslensk netlögsaga:* Net sem falla innan þeirra raða IP-vistfanga sem hefur verið úthlutað til íslenskra aðila.
2. *Nafnlaus rauntímagögn:* Tölulegar upplýsingar og kóðar sem bjóða upp á rekjanleika fjarskiptaumferðar í IP-fjarskiptanetum.
3. *Netöryggissveit Póst- og fjarskiptastofnunar* eða *netöryggissveitin* (CERT-ÍS): Öryggis- og viðbragðshópur sem starfar á vegum Póst- og fjarskiptastofnunar til verndar ómissandi upplýsingainnviðum gegn netárásum.
4. *Net- og upplýsingaöryggi:* Hæfni fjarskiptaneta til að tryggja að ákveðin fyrirfram skilgreind öryggismörk standist þegar ógnir steðja að eða ef veilur myndast, t.d. vegna mannlegra mistaka eða skemmdarverka, sem stofna í hættu leynd, réttleika og tiltækileika upplýsinga í fjarskiptanetum. Það getur auk þess falið í sér aðra eiginleika, svo sem ósvikni, ábyrgni, óhrekjanleika og áreiðanleika.
5. *Netumdæmi:* Sjálfstæð eða eftir atvikum samtengd fjarskipta- og/eða upplýsingakerfi á vegum þjónustuhópsins, þ.m.t. rekstraraðila ómissandi upplýsingainnviða, sem hafa gert þjónustusamning við netöryggissveitina um ráðgjöf, aðstoð og viðbúnað til að verjast mögulegum netárásum á kerfin sem gerðar eru í þeim tilgangi að gera þau óvirk, valda skemmdum á þeim eða til öflunar ólögmæts fjárhagslegs ávinnings, svo sem með þjófnaði á gögnum eða peningum.
6. *Ómissandi upplýsingainnviðir:* Upplýsingakerfi þeirra mikilvægu samfélagslegu innviða sem tryggja eiga þjóðaröryggi, almannaheill og margs konar öflun aðfanga í þróuðu og tæknivæddu þjóðfélagi. Um er að ræða þann tækja- og hugbúnað sem nauðsynlegur er til reksturs og virkni kerfisins og þær upplýsingar sem þar eru hýstar eða um kerfið fara. Ríkislögreglustjóri skilgreinir ómissandi upplýsingainnviði.
7. *Viðbúnaðarstig 1:* Óvissa vegna öryggisatviks sem gæti valdið ógn gagnvart rekstrarhæfni ómissandi upplýsingainnviða og getur hugsanlega valdið tjóni eða þjónusturofi, þótt ekki liggi fyrir endanleg þekking á skaðlegri virkni öryggisatviksins né mögulegu umfangi þess.
8. *Viðbúnaðarstig 2:* Hættuástand vegna öryggisatviks sem hefur haft skaðleg áhrif á rekstrarhæfni eins eða fleiri ómissandi upplýsingainnviða eða mun að öllum líkindum hafa skaðleg áhrif á slíka innviði með ófyrirséðum afleiðingum.
9. *Viðbúnaðarstig 3:* Neyðarástand vegna öryggisatviks sem hefur raungerst og haft alvarleg áhrif á rekstrarhæfni ómissandi upplýsingainnviða, valdið miklu tjóni eða fyrirsjáanlega getur valdið miklu tjóni, tafið eða hamlað endurræsingu kerfis, eða umfang öryggisatviksins nær til fleiri en eins ómissandi upplýsingainnviða.
10. *Þjónustuhópur netöryggissveitarinnar* eða *þjónustuhópurinn:* Hópurinn samanstendur annars vegar af fjarskiptafyrirtækjum sem reka almenn fjarskiptanet og/eða veita aðgang að internetinu

og internetþjónustu og hins vegar rekstraraðilum ómissandi upplýsingainnviða sem samkvæmt sérstökum þjónustusamningi við netöryggissveitina gerast meðlimir þjónustuhópsins. Viðeigandi net þjónustuhópsins mynda svonefnt netumdæmi og öryggisatvik innan þess njóta forgangs til þeirrar þjónustu sem netöryggissveitin veitir.

11. *Öryggisatburður:* Það að upp kemur staða kerfis, þjónustu eða nets sem gefur til kynna hugsanlegt brot gegn öryggisstefnu viðkomandi eða bilun í öryggisráðstöfun, eða þá áður óþekkt staða sem getur skipt máli fyrir öryggi.
12. *Öryggisatvik:* Atvik sem er gefið til kynna með einum eða fleiri óæskilegum eða óvæntum öryggisatburðum sem talsverðar líkur eru á að stofni rekstrarþáttum í hættu og ógni upplýsingaöryggi.

3. gr.

Netumdæmi og íslensk netlögsaga.

Netöryggissveitin gegnir hlutverki landstengiliðs vegna netöryggisatvika innan íslenskrar netlögsögu (e. national point of contact).

Starfssvæði netumdæmis sveitarinnar tekur til ómissandi net- og tæknikerfa íslenskra fjarskiptafyrirtækja og samkvæmt sérstökum þjónustusamningum við rekstraraðila ómissandi upplýsingainnviða landsins, bæði þeirra sem tengjast internetinu á einn eða annan hátt, sem og þeirra sem eru í vissum tilfellum með búnað sem er alfarið ótengdur við netið t.d. iðnstýringar. Vinna sveitarinnar innan netumdæmisins er í forgangi. Sé hluti búnaðar í netumdæminu í rekstri á erlendri grundu, fellur hann eftir atvikum undir verksvið sveitarinnar.

II. KAFLI
Skipulag, hlutverk og verkefni.

4. gr.

Skipulag og hlutverk.

Netöryggissveitin CERT-ÍS er staðsett innan Póst- og fjarskiptastofnunar. Forstjóri Póst- og fjarskiptastofnunar skiptir verkum og ábyrgð milli starfsmanna netöryggissveitarinnar. Rekstur netöryggissveitar skal bókhaldslega aðgreindur frá öðrum rekstri stofnunarinnar. Netöryggissveitin skal starfa í samræmi við gæðastefnu stofnunarinnar.

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.

5. gr.

Hæfiskröfur starfsmanna.

Póst- og fjarskiptastofnun skal gera viðeigandi ráðstafanir við skipun starfsmanna netöryggissveitarinnar, til þess að tryggja hæfi starfsmanna, sérstaklega með tilliti til vinnslu viðkvæmra upplýsinga, svo og trúnaðarflokkaðra upplýsinga sem geta komið fram við margs konar úrvinnslu. Geta þær ráðstafanir m.a. falist í öryggisvottun starfsmanna netöryggissveitarinnar af hálfu ríkislögreglustjóra. Um öryggisvottanir af hálfu ríkislögreglustjóra fer samkvæmt lögum þar um.

6. gr.

Verkefni netöryggissveitarinnar.

Helstu verkefni netöryggissveitarinnar eru að:

1. stuðla að vernd ómissandi upplýsingainnviða, samkvæmt þar til gerðum þjónustusamningum;
2. vakta upplýsingainnviði rekstraraðila sem hafa gert þjónustusamning við netöryggissveitina gagnvart ógnunum og meta hvort grípa þurfi til ákveðinna viðbúnaðaraðgerða;

3. móta og efla ástandsvitund um atvik og ógnir. Fylgst er með stöðunni hérlendis frá degi til dags með skráningu atvika hérlendis og skoðun á mynstri fjarskiptaumferðar fjarskiptafyrirtækjanna í stjórnstöð sveitarinnar. Ennfremur að vakta ógnir sem steðja að Íslandi og meta hvort grípa þurfi til ákveðinna viðbúnaðaraðgerða. Þessum upplýsingum um stöðu mála er miðlað áfram, og fer það eftir eðli þeirra hvert og hvernig;
4. ná sem best tökum á öryggisatvikum og meðhöndla þau til að takmarka mögulegt tjón. Við alvarleg öryggisatvik er sveitin jafnframt samhæfingaraðili innan íslenskrar netlögsögu;
5. vera landstengiliður um CERT-málefni og málefni ómissandi upplýsingainnviða þar á meðal þegar æfingar eru haldnar o.s.frv. Í þessu felst m.a. norrænt og annað alþjóðlegt samstarf á þessu sviði, t.d. um að skiptast á gögnum um öryggisatvik, gefa upplýsingar um varnir og viðbúnað. Sum þessara gagna geta varðað trúnaðarflokkaðar upplýsingar, sbr. 19. gr.;
6. veita margs konar ráðgjöf um aðgerðir og viðbúnað, fyrst og fremst til þjónustuhópsins, en einnig til stjórnsýslunnar, almennings og annarra ef svo ber undir. Sveitin kemur jafnframt að mótun skipulags, gerð viðbúnaðaráætlunar fyrir landið í heild o.fl.;
7. vera virkur þátttakandi í margs konar átaksverkefnum hérlendis, t.d. með því að setja á laggirnar samráðsvettvang og skipuleggja samstarf um yfirvofandi hættur þegar á þarf að halda;
8. skipuleggja og koma á netæfingum sem fyrst og fremst snúa að ómissandi upplýsingainnviðum en geta teygt sig víðar í þjóðfélaginu, sem og æfingum í samstarfi við erlenda aðila.

Einstök verkefni netöryggissveitarinnar kunna að skarast að hluta við starfsemi og þjónustu einkaaðila. Það kemur þó ekki í veg fyrir að sveitin sinni framangreindum verkefnum, enda séu þau unnin í tengslum við heildstæðan viðbúnað á vegum hins opinbera til að efla og samræma aðgerðir um vernd ómissandi upplýsingainnviða.

Sveitin skal eftir þörfum beita verklagi sem fastmótar vinnubrögð og hugtök. Henni er ekki skylt að gera verklag sitt opinbert, svo fremi að leyndin sé nauðsynleg vegna almannahagsmuna, þjóðaröryggis og skipulags varnarmála, sbr. 1. tölulið 10. gr. upplýsingalaga nr. 140/2012.

III. KAFLI
Aðgerðir, samhæfing og samstarf.

7. gr.
Stjórn öryggisatvika.

Netöryggissveitin vinnur að því að efla þá umgjörð sem stuðlar að öflugri starfsemi og bættu netöryggi, svo sem skipulagi, ráðgjöf um lagaumhverfi o.fl. Kjarni starfseminnar felst þó í því að greina og meta öryggisatvik, sem og að leiðbeina um mótaðgerðir sem þjónustuhópurinn að öllu jöfnu hrindir af stað með það að markmiði að lágmarka áhrif atvika.

Með aðilum innan og, eftir atvikum, utan þjónustuhópsins, er sveitinni heimilt að leiða margs konar undirbúning, forvarnarstarf og koma að mótun skipulags viðbúnaðar hérlendis. Skal það gert í samstarfi við aðra viðeigandi viðbragðsaðila eftir því sem kostur er. Sveitin skal koma að mótun áhættustýringar, innleiðingu o.fl. því tengt, við vernd ómissandi upplýsingainnviða landsins sem ráðuneyti og stofnanir leiða. Sveitinni er að auki heimilt að vinna að stefnumótun um netöryggi, við samræmda og heildstæða viðbúnaðaráætlun fyrir landið allt, víðtækt áhættumat o.s.frv.

Þá er sveitinni heimilt, með samþykki rekstraraðila ómissandi upplýsingainnviða, að hafa beina aðkomu að skipulagi og stjórnun órofa reksturs, sem og áætlun um endurreisn viðkomandi upplýsingainnviða.

Í yfirlitsskýrslu sveitarinnar sem gefin skal út a.m.k. árlega skal höfuðáhersla lögð á öryggisatvik og ógnir.

8. gr.
Samhæfing aðgerða í netumdæminu og utan þess.

Netöryggissveitin samhæfir aðgerðir gagnvart öryggisatvikum innan þjónustuhópsins. Sveitinni er heimilt að samhæfa aðgerðir aðila utan þjónustuhópsins samkvæmt sérstakri beiðni viðkomandi.

Skal þá leitast við að viðkomandi undirriti þjónustusamning við netöryggissveitina, enda leyfi tími og aðstæður slíkt.

Er netöryggissveitinni heimilt að forgangsraða verkefnum á þessu sviði, svo sem þegar fleiri en eitt alvarlegt öryggisatvik á sér stað.

9. gr.

Viðbúnaðarstig vegna öryggisatvika.

Eftir aðstæðum virkjar netöryggissveitin viðbúnaðarstig vegna öryggisatvika og skiptast þau í þrjú stig, þ.e. viðbúnaðarstig 1, viðbúnaðarstig 2 og viðbúnaðarstig 3. Netöryggissveitin setur verklagsreglur með viðmiðum til nánari aðgreiningar á mismundi viðbúnaðarstigum. Skulu þær m.a. greina frá umfangi hvers stigs fyrir sig með nauðsynlegum skipulagslegum aðgerðum vegna þeirra. Ef þörf er á boðar sveitin til neyðarsamráðs viðeigandi þjónustuhóps og sér um fyrirkomulag og skipulag þess.

10. gr.

Skipulag og viðbúnaður vegna viðbúnaðarstiga.

Viðbúnaðarstig 1.

Netöryggissveitin viðhefur nauðsynlegar ráðstafanir til þess að gera viðeigandi aðilum þjónustuhópsins viðvart og metur hvort hefja þurfi neyðarsamráð.

Viðbúnaðarstig 2.

Netöryggissveitin boðar til neyðarsamráðs til ákvörðunar um skipulögð og samhæfð viðbrögð til verndar rekstrarhæfni ómissandi upplýsingainnviða og til að sporna gegn frekari útbreiðslu öryggisatviks.

Viðbúnaðarstig 3.

Aðstæður kalla á fullan viðbúnað netöryggissveitarinnar innan netumdæmisins og eftir atvikum, samstarf við erlenda samstarfsaðila og aðra aðila hér innanlands. Viðeigandi aðilar þjónustuhópsins skulu eftir fremsta megni taka tillit til tilmæla netöryggissveitarinnar um aðgerðir sem ræddar hafa verið í neyðarsamráðinu, eða almennra tilmæla sem sveitin eða Póst- og fjarskiptastofnun sendir frá sér að eigin frumkvæði. Netöryggissveitinni er heimilt að leita til embættis ríkislögreglustjóra og eftir atvikum innanríkisráðherra, til að knýja fram tilteknar aðgerðir, enda gefi alvarleiki og umfang öryggisatviksins tilefni til þess.

11. gr.

Upplýsingagjöf og samstarf við ríkislögreglustjóra.

Netöryggissveitin skal halda ríkislögreglustjóra upplýstum um öryggisatvik sem hafa alvarleg áhrif á rekstrarhæfni eins eða fleiri ómissandi upplýsingainnviða. Netöryggissveitinni er skylt að tilkynna ríkislögreglustjóra um þegar viðbrögð við öryggisatviki færast frá viðbúnaðarstigi 2 yfir á viðbúnaðarstig 3.

Nú hefur netöryggissveitin fengið upplýsingar um uppruna alvarlegrar netárásar eða gerendur að baki öryggisatviks sem valdið hefur tjóni og/eða háttsemin kann að brjóta í bága við ákvæði almennra hegningarlaga, fjarskiptalaga eða annarra laga er netöryggissveitinni heimilt, að höfðu samráði við rekstraraðila þeirra ómissandi upplýsingainnviða sem hlut eiga að máli, að tilkynna ríkislögreglustjóra og/eða viðkomandi lögreglustjóra um meint brot og umfang þess. Um frekari gagnaöflun lögregluyfirvalda fer samkvæmt heimildum í lögum.

12. gr.

Hlutverk ríkislögreglustjóra.

Telji ríkislögreglustjóri að alvarlegt öryggisatvik varði almannahagsmuni og/eða þjóðaröryggi lýsir hann yfir almannavarnaástandi. Samhæfing, mat á stöðu og ákvörðun um viðeigandi aðgerðir fer þá samkvæmt lögum nr. 82/2008 um almannavarnir, eftir því sem við á.

Hlutverk og verkefni netöryggissveitarinnar í almannavarnaástandi skulu vera skilgreind í viðbragðsáætlun ríkislögreglustjóra um netvá sem unnin skal í samráði við sveitina.

Skipting aðgerða netöryggissveitarinnar í mismunandi viðbúnaðarstig, samkvæmt 9. gr. reglugerðarinnar, kemur ekki í veg fyrir að ríkislögreglustjóri geti hvenær sem er, að eigin frumkvæði, lýst yfir almannavarnaástandi vegna netöryggisvár.

13. gr.

Almennt samstarf utan öryggisatvika.

Netöryggissveitinni er heimilt að setja á laggirnar samstarfshópa mismunandi hluta þjónustuhópsins til að efla forvarnir og þegar bregðast þarf við öryggisatvikum.

Hlutverk netöryggissveitarinnar er að efla samstarf þjónustuhópsins, m.a. með því að boða til reglulegra funda. Netöryggissveitin tekur ákvörðun um boðun slíkra samstarfshópa og er sveitinni jafnframt heimilt að leita eftir ráðgjöf og samstarfi um netöryggismál til utanaðkomandi aðila. Fundunum er stýrt af fulltrúa netöryggissveitarinnar og þeir haldnir í húsakynnum völdum af netöryggissveitinni. Í sama tilgangi er netöryggissveitinni heimilt að nýta sér fjarskiptatækni, svo sem fjarfundi.

Til að styrkja samstarfið er netöryggissveitinni heimilt skv. beiðni frá viðkomandi, að framkvæma eða láta gera úttektir á net- og upplýsingaöryggi, hjá aðilum innan netumdæmisins. Skal viðkomandi greiða fyrir útlagðan kostnað við slíka úttekt. Einnig er sveitinni heimilt að halda eða skipuleggja kynningar og ráðstefnur og að skapa umræðuvettvang þessara aðila.

Netöryggissveitinni er heimilt að vinna með öðrum CERT-sveitum á Íslandi og gera við þá þjónustusamninga. Sömu reglur gilda um gjaldtöku fyrir þá aðila sem ekki flokkast sem ómissandi upplýsingainnviðir.

Undir starfsemi sveitarinnar heyrir alþjóðlegt samstarf um aðgerðir t.d. við erlenda systurhópa og aðra tengda aðila um málefni CERT-netöryggissveita, málefni ómissandi upplýsingainnviða og önnur tengd mál.

14. gr.

Þjónustusamningar.

Þjónustusamningar sem sveitin gerir skulu innihalda lýsingu á þeirri grunn- og viðbótarþjónustu sem veitt er, gjaldtöku, kostnaði vegna sérstaks búnaðar sem settur er upp á neti viðkomandi, upplýsingar um tengiliði, gagnkvæman trúnað o.fl.

Þar skulu einnig koma fram skilyrði gagnvart samningsaðila varðandi upplýsingar um gjaldtöku, meðal svar- og viðbragðstíma sveitarinnar, gagnkvæma upplýsingagjöf, um vaktir og bakvaktir og tengiliði.

Með gerð þjónustusamnings skuldbindur rekstraraðili ómissandi upplýsingainnviða sig til að taka eftir fremsta megni tillit til ráðgjafar netöryggissveitarinnar um stjórnskipulag upplýsingaöryggis, verkferla, eftirlit og úttektir á öryggi net- og upplýsingakerfa. Einnig nær skuldbindingin til að taka virkan þátt í öðru samstarfi svo sem netvarnaræfingum og öðrum viðbúnaði.

IV. KAFLI
Móttaka, meðferð og miðlun gagna.

15. gr.

Almennt.

Netöryggissveitinni er heimilt:

að taka á móti, greina innihald og meta gögn og upplýsingar sem sveitinni eru sendar vegna meintra öryggisatvika, þ. á m. gögn frá öðrum CERT-netöryggissveitum. Gögn þessi geta verið margs konar, t.d. lýsing á öryggisatviki eða meintu öryggisatviki, viðvörun þar um, hverjir standi að því og/eða innihald þess svo sem eintak af tilheyrandi spilliforriti.

að miðla þessum gögnum áfram til viðkomandi aðila innan netumdæmisins og til samstarfsaðila netöryggissveitarinnar. Skulu viðtakendurnir gæta skipulags og tækni til að tryggja sem best öryggi gagnanna og trúnað gagnvart netöryggissveitinni.

að móttaka og vinna hliðstætt með önnur gögn sem snerta netviðbúnað og skipulag á landsvísu og alþjóðavettvangi. Gögn þessi snerta m.a. ómissandi upplýsingainnviði, stefnumótandi drög og ákvarðanir og önnur skjöl, hvort sem er hérlendis eða í alþjóðlegu samstarfi.

að tilkynna atvik til ríkislögreglustjóra, ef atvik varðar almanna- eða þjóðaröryggi. Varði slíkt tilvik þjóðaröryggi er sveitinni aðeins heimilt að gera það opinbert að fengnu samþykki frá ríkislögreglustjóra.

Sem landstengiliður er netöryggissveitin sá aðili sem hægt er að leita til, ef aðrar leiðir hafa ekki reynst færar við að koma gögnum og ýmsum upplýsingum um meint öryggisatvik áleiðis til viðkomandi aðila hérlendis.

Við flutning og úrvinnslu gagna og upplýsinga er netöryggissveitinni heimilt að nýta sér tækni hvers tíma, svo sem tölvupóst, lokaðar miðlunarrásir, eða aðrar leiðir.

16. gr.

Meðhöndlun gagna og gagnalýsing.

Til þess að rækja hlutverk sitt er netöryggissveitinni heimilt að greina, miðla áfram og vinna tölfræði úr fyrirliggjandi nafnlausum gögnum eða meðhöndla á annan hátt, og í framhaldi benda þjónustuhópnum á eða óska eftir tilteknum aðgerðum af þeirra hálfu í ljósi ákveðinnar hættu.

Í gögnum um öryggisatvik er oft stuðst við IP-upplýsingar, svo sem IP-tölur, hliðnúmer o.fl. Netöryggissveitinni er því heimilt að vinna með og meðhöndla IP-vistföng og önnur gögn í haus IP-fjarskiptapakka.

Netöryggissveitinni er að öðru leyti óheimilt að persónugreina nafnlaus umferðargögn sem skimuð eru rafrænt eða safnað, svo sem með því að samkeyra upplýsingar um IP-vistföng við skrár yfir áskrifendur. Er fjarskiptafyrirtækjum og internetþjónustuaðilum óheimilt að afhenda netöryggissveitinni skrár yfir áskrifendur.

Leiki grunur á um stórfellda netárás er netöryggissveitinni heimilt að skima stýrigögn fjarskiptapakka sem tengjast hugsanlegum öryggisógnum með tilliti til nánari upplýsinga um uppruna, áfangastað og tæknilega eiginleika. Eingöngu má nota gögn sem þannig er aflað í þeim tilgangi að koma í veg fyrir eða draga úr tjóni öryggisatvika. Óheimilt er að persónugreina upplýsingar sem aflað er samkvæmt þessari grein og skal þeim eytt eins fljótt og auðið er en þó eigi síðar en sex mánuðum frá því að þeirra var aflað.

Aðilum þjónustuhópsins er heimilt að vinna úr upplýsingum sem netöryggissveitin miðlar til þeirra og grípa til þeirra nauðsynlegu öryggisráðstafana sem hún leggur til. Slíkar ráðstafanir geta m.a. falist í því að hafa samband við aðila utan netumdæmisins, þ.m.t. við hugsanlega endanotendur eða áskrifendur, til að mynda ef gera þarf viðvart um yfirvofandi hættu.

17. gr.

Skoðun á efnisinnihaldi sendinga í ómissandi upplýsingainnviðum.

Leiki rökstuddur grunur um að einstakar sendingar innihaldi spillikóta er netöryggissveitinni heimilt, með samþykki rekstraraðila einstakra ómissandi upplýsingainnviða, að greina efni einstakra fjarskiptasendinga til og frá viðkomandi neti. Þessi heimild tekur þó ekki til skoðunar sendingar í almennum fjarskiptanetum fjarskiptafyrirtækja. Tilkynna skal sendanda og móttakanda sendingarinnar um að hún verði skoðuð og gefa þeim tækifæri á því að vera viðstaddir skoðunina ef það er mögulegt. Að öðru leyti skal netöryggissveitin starfa í samræmi við skilyrði sem Persónuvernd kann að setja fyrir vinnslunni.

Netöryggissveitin skal setja sér verklag við slíka skoðun, þar sem fram kemur hvernig eigi að láta ábyrgðaraðila sendinga vita áður en skoðun fer fram. Nú ber svo við að ekki er raunhæft eða nægjanlegur fyrirvari til að tilkynna slíkt og skulu þær undanþágur koma fram í verklaginu.

Til að tryggja sem best friðhelgi einkalífs, skal eyða gögnum sem safnað er og skoðuð á þennan hátt innan sex mánaða frá því að þeirra var aflað. Þegar söfnuðum eða skoðuðum gögnum er eytt, skal það gert á sem öruggastan hátt þar sem ekki verða skilin eftir nein afrit.

18. gr.

Innlendar tilkynningar og viðbrögð.

Fái netöryggissveitin upplýsingar um tiltekna hættu eða öryggisatvik sendir hún tilkynningu til ábyrgðaraðila viðkomandi fjarskiptanets eða tengipunkts/léns sé talin brýn ástæða til.

Við slíka tilkynningu skal netöryggissveitin eftir bestu getu ganga úr skugga um að undirliggjandi forsendur séu traustar og tilkynningar eða viðvaranir sem hún sendir frá sér séu á rökum reistar, séu til gagns, nægjanlega ítarlegar og heilsteyptar.

Í því skyni að tryggja áreiðanleika upplýsinga er sveitinni heimilt að eiga samskipti við þjónustur á netinu er málið varða, svo fremi þær séu opinberlega aðgengilegar og ekki aðgangsstýrðar.

Sveitin getur flokkað tilkynningar í aðgerðaflokka, til þess að ekki sé mismunandi skilningur móttakenda á umbeðnum aðgerðum. Skal notkun móttakenda einvörðungu bundin við það öryggisatvik sem við á, eða afleiðu þess.

Ef í ljós kemur, m.a. við endurtekin tilvik að ekki hefur verið gripið til umbeðinna aðgerða hérlendis, er netöryggissveitinni heimilt að beita frekari úrræðum Póst- og fjarskiptastofnunar, eða leita til ríkislögreglustjóra og/eða viðkomandi lögreglustjóra um að gripið verði til viðeigandi aðgerða innan eða utan þjónustuhópsins.

19. gr.

Tilkynningar til erlendra samstarfsaðila.

Hafi netöryggissveitin upplýsingar um öryggisatvik sem viðkemur erlendu fjarskiptaneti hefur sveitin heimild til að miðla upplýsingum um það til erlendra samstarfsaðila. Feli slík gögn í sér persónugreinanlegar upplýsingar skal miðlun þeirra uppfylla skilyrði 29. gr. eða eftir atvikum 30. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Slík miðlun skal hafa það að markmiði að leysa úr viðkomandi öryggisatviki og áhrifum þess.

20. gr.

Öryggisráðstafanir.

Til að tryggja öryggi innsendra gagna sem best, skal netöryggissveitin leitast við að gefa sendanda kost á að senda þau á sem öruggastan hátt miðað við tækni hverju sinni, svo sem með dulkóðun, rafrænni undirritun o.s.frv.

Ennfremur skal netöryggissveitin leitast við að tryggja sem best öryggi gagna sem sveitin vinnur með hverju sinni, eða geymir í sinni vörslu, með aðgangsstýringum, dulritun eða öðrum tiltækum öryggisráðstöfunum hvers tíma.

Gögn um öryggisatvik skal netöryggissveitin ekki geyma lengur en þörf er á vegna viðbragða, málsskráningar eða skýrslugerðar. Skal sveitin setja sér verklagsreglur sem taka til líftíma og eyðingu gagna miðað við flokkun þeirra.

Netöryggissveitin skal gera öryggisráðstafanir þegar sendar eru tilkynningar um öryggisatvik til að tryggja eftir fremsta megni trúnaðarstig tilkynninganna. Að sama skapi skulu viðtakendur slíkra tilkynninga virða trúnaðarstig þeirra og viðhafa nægjanlegar tæknilegar ráðstafanir og verkferla til þess.

Þegar trúnaðarupplýsingar sem falla undir reglugerð um vernd trúnaðarupplýsinga, öryggisvottanir og öryggisviðurkenningar á sviði öryggis- og varnarmála nr. 959/2012 eiga í hlut skal viðeigandi húsnæði, aðgengi og verklag, vera viðurkennt af ríkislögreglustjóra í samræmi við þá reglugerð.

V. KAFLI
Umferðarmælingar.

21. gr.

Framkvæmd umferðarmælinga.

Netöryggissveitinni er heimilt að setja upp eftirlitsbúnað í þeim tilgangi að greina snögga breytingu í magni á umferð nafnlausra rauntímagagna hjá fjarskiptafyrirtækjum sem gæti bent til að gerð sé netárás á innviði á Íslandi eða frá Íslandi. Sveitinni er heimilt að nýta tölfræði úr þessum gögnum og er geymslutími slíkra gagna án takmarkana. Frumgögnum skal eyða í samræmi við ákvæði um geymslutíma gagna í fjarskiptalögum.

Ef við mælingar í eftirlitsbúnaði myndast rökstuddur grunur um stórfellda netárás er sveitinni heimilt, eftir að hafa lýst yfir skilgreindu viðbúnaðarstigi, að óska eftir að opnaður sé tímabundið aðgangur að lifandi umferðargögnum sem málið varða hjá viðkomandi fjarskiptafyrirtæki, svo sem á

hvaða IP-vistföng mestri umferð er beint hverju sinni og hvaðan megnið af þeirri umferð kemur. Um meðhöndlun og skimun slíkra gagna fer skv. 16. og 17. gr. Skal slíkum frumgögnum eytt innan 3ja vikna en geymsla tölfræðigagna er án takmarkana.

22. gr.

Tenging við umferðarmælibúnað.

Tenging eða tengingar eftirlitsbúnaðar stjórnstöðvar netöryggissveitarinnar við umferðarmælibúnað tiltekins fjarskiptafyrirtækis sem sveitin ákveður að tengjast, skal vera á kostnað viðkomandi fjarskiptafyrirtækis, bæði hvað varðar rekstur og uppsetningu, þar með talið virkur endabúnaður og fjöldi tenginga. Allt þetta skal vera í samræmi við óskir sveitarinnar er lýtur að gerð, umferðargetu og öðru sem nauðsynlegt þykir til að gagnaflutningurinn gangi snurðulaust fyrir sig. Leitast skal við að nota þann búnað sem fyrir er hjá fjarskiptafyrirtækjum ef mögulegt er.

23. gr.

Eftirlit með umferðarmælingum.

Póst- og fjarskiptastofnun hefur eftirlit með því að farið sé eftir ákvæðum þessarar reglugerðar er lýtur að umferðarmælingum innan fjarskiptafyrirtækja í samræmi við ákvæði 47. gr. a í lögum um fjarskipti nr. 81/2003.

Fjarskiptafyrirtækjum og birgjum er skylt að veita Póst- og fjarskiptastofnun allar þær upplýsingar sem stofnuninni eru nauðsynlegar vegna eftirlits með ákvæðum laga og reglugerðar þessarar og á því formi sem stofnunin áskilur vegna gagnöflunar.

Póst- og fjarskiptastofnun getur m.a. aflað upplýsinga um fjölda mælitækja, frávika sem koma fram við prófanir og önnur þau atriði sem nauðsynleg eru vegna eftirlits með umferðarmælingum.

24. gr.

Skimun umferðar hjá ómissandi upplýsingainnviðum.

Netöryggissveitinni er heimilt að setja upp nema sem greina innihald umferðar við tengihlið rekstraraðila ómissandi upplýsingainnviða, sem gert hafa þjónustusamning við netöryggissveitina, eða annarra aðila sem um það biðja. Þetta gildir þó ekki um fjarskiptafyrirtæki er snýr að rekstri almennra fjarskiptaneta þeirra. Gera skal samning milli sveitarinnar og viðkomandi um þessa þjónustu og annað henni tengt skv. fjarskiptalögum. Geymslutími frumgagna skal vera tilgreindur í þeim samningi. Sveitinni er sömuleiðis heimilt að greina úr gögnunum skrár, forrit og annað er inniheldur ópersónugreinanlegar tölvuveirur og/eða annan spillikóða og að geyma slík sýnishorn og miðla áfram til systurhópa og þriðja aðila til frekari rannsóknar. Geymslutími slíkra gagna er án takmarkana.

VI. KAFLI
Um ábyrgð og skyldur gagnvart tilkynningum.

25. gr.

Fjarskiptafyrirtæki.

Fjarskiptafyrirtæki skal vakta og móttaka tilkynningar og aðrar upplýsingar sem netöryggissveitin sendir frá sér og vinna úr þeim eins fljótt og auðið er í samræmi við flokkun sveitarinnar á aðgerðarstigi. Í því felst uppsetning, rekstur og viðhald nauðsynlegs búnaðar og innri verkferla til að framfylgja tilmælunum á markvissan hátt.

Fjarskiptafyrirtæki ber ábyrgð á þeim aðgerðum sem það grípur til innan sinna fjarskiptaneta, skv. tilmælum sveitarinnar þar um. Því er heimilt að bregðast við tilmælum sveitarinnar skv. flokkun tilkynninga og í einstökum tilkynningum ef svo ber undir, svo sem með viðvörun, lokun að hluta eða tímabundið o.fl. Skal þessi fyrirvari koma skýrt fram í viðskiptamannasamningum fjarskiptafyrirtækjanna við viðskiptavini sína.

Fjarskiptafyrirtæki skal senda netöryggissveitinni upplýsingar um þau öryggisatvik sem það verður áskynja, innan þeirra raða IP-vistfanga sem falla undir ábyrgð fjarskiptafyrirtækisins skv. samningi þess við þann aðila sem úthlutaði vistföngunum. Gildir einu hvort meint atvik sé ekki rekjanlegt til IP-vistfanga, t.d. tengist spilliforritum, blekkingum eða netárásum frá ókunnum upp-

runa, eða öðrum öryggisatvikum sem stofnað er til af ásetningi með net- og tölvutækni. Skal netöryggissveitin útbúa eyðublað eða nota rafrænar leiðir til móttöku slíkra tilkynninga sem skulu mótaðar í samráði við fjarskiptafyrirtæki.

Fjarskiptafyrirtæki skal gefa sveitinni yfirlitsskýrslu árlega og eigi síðar en 1. febrúar hvert ár um öll atvik síðastliðins árs. Yfirlitsskýrslan skal gefa tölfræðilegt yfirlit um allar gerðir öryggisatvika og annað sem skipt getur máli. Form hennar skal vera eins og sveitin ákveður.

26. gr.

Aðilar utan þjónustuhópsins.

Öðrum aðilum, svo sem iðnfyrirtækjum, fréttamiðlum og hugbúnaðarframleiðendum sem ekki hafa gert þjónustusamning við CERT-ÍS, er heimilt að senda til netöryggissveitarinnar margs konar gögn og upplýsingar, svo sem um meiri háttar atvik sem upp koma í netum þeirra, t.d. um netárásir sem trufla rekstur. Skulu fylgja með í tilkynningunni upplýsingar um hvort viðkomandi vilji eða vilji ekki að viðkomandi atvik verði gert opinbert. Netöryggissveitinni er heimilt að nota allar slíkar upplýsingar í tölfræði sbr. 16. gr. og til frekari vinnslu og birtingar. Upplýsingar sem sveitin verður áskynja um á þennan hátt má eingöngu nota í þeim tilgangi að koma í veg fyrir eða draga úr tjóni öryggisatvika.

VII. KAFLI
Kæruheimild, viðurlög og gildistaka.

27. gr.

Kæruheimild.

Ákvörðun sem netöryggissveit Póst- og fjarskiptastofnunar tekur á grundvelli þessarar reglugerðar má kæra til úrskurðarnefndar fjarskipta- og póstmála, sbr. 13. gr. laga nr. 69/2003 um Póst- og fjarskiptastofnun.

28. gr.

Viðurlög.

Sá sem af ásetningi eða gáleysi brýtur gegn ákvæðum reglugerðar þessarar skal sæta viðurlögum í samræmi við 74. gr., sbr. og 73. gr. laga um fjarskipti nr. 81/2003.

29. gr.

Gildistaka.

Reglugerð þessi tekur gildi 1. júní 2013.

Reglugerðin er sett með stoð í 6. mgr. 47. gr. a, laga nr. 81/2003 um fjarskipti, sbr. 6. mgr. 8. gr. laga nr. 62/2012 til breytinga á fjarskiptalögum, auk 75. gr. laga um fjarskipti nr. 81/2003.

Innanríkisráðuneytinu, 26. apríl 2013.

Ögmundur Jónasson.

Ragnhildur Hjaltadóttir.

B-deild – Útgáfud.: 23. maí 2013