Fjarskiptastofa

Ákvörðun nr. 2/2024

Öryggisatvik hjá Símanum hf.

(mál nr. 2021120010)

I. Almennt

(1) Þann 12. október 2021 kom upp öryggisatvik hjá Símanum hf. (hér eftir Síminn). Barst Fjarskiptastofu frávikaskýrsla um atvikið strax í kjölfarið.

(2) Fjarskiptastofa hóf forskoðun á öryggisatvikinu með bréfi dags, 9. desember 2021. Í kjölfar öflunar upplýsinga frá Símanum var það niðurstaða stofnunarinnar að hefja stjórnsýsluskoðun á umræddu öryggisatviki. Var félaginu tilkynnt um þá niðurstöðu með bréfi, dags. 6. maí 2022 ásamt því að frekari upplýsinga var aflað.

II. Forskoðun öryggisatviks hjá Símanum

2.1 Öryggisatvik

(3) Þann 12. október 2021 kl. 11:30 - 12:02 varð rof á farsíma- og farnetsþjónustu Símans og á hluta fastlínukerfa Símans. Strax hafði rofið veruleg áhrif á farsímanotendur og var fjallað um það í fréttum fjölmiðla[1]. Þann 19. október barst Fjarskiptastofu frávikaskýrsla frá atvikastjórn Símans um öryggisatvikið. Í lýsingu á öryggisatvikinu í frávikaskýrslu segir:

> *Farsímakjarni Símans […][2]. Stór hluti kerfisins keyrir í […][3] sem framleiðandi kerfisins er að uppfæra í […][4] og á meðan er umferð að keyra í […][5]. Vinna við uppfærsluna er*

[1] https://www.mbl.is/frettir/innlent/2021/10/12/vidtaek_truflun_vegna_mannlegra_mistaka/
[2] Hluti frávikaskýrslu ekki birt opinberlega.
[3] Hluti frávikaskýrslu ekki birt opinberlega.
[4] Hluti frávikaskýrslu ekki birt opinberlega.
[5] Hluti frávikaskýrslu ekki birt opinberlega.

að klárast þessa dagana og verið er að keyra aftur upp sýndarvélar í […][6]. Við þá vinnu komu upp vandamál […][7] sem geymir upplýsingar um farsímanotendur. […][8]. Til að laga það vandamál, þá voru gerðar breytingar […][9] en þær configbreytingar voru óvart […][10]. Það hafði þau áhrif að […][11] varð óaðgengilegur fyrir símstöðvar í […][12]. Þetta voru mannleg mistök hjá framleiðanda kerfisins. Áhrifin voru þau að flest símtöl farsímaviðskiptavina virkuðu ekki. Einnig fóru notendur að detta af farsímanetinu þegar reglubundnar auðkenningar notenda virkuðu ekki sem skildi.

(4) Þá segir í frávikaskýrslunni varðandi fyrirbyggjandi aðgerðir:

Farið yfir ferla með framleiðanda búnaðarins. Allar configbreytingar skoðaðar í þaula og allar breytingar sem hugsanlega hafa áhrif á notendur skulu gerðar að nóttu til eins og venjan er hjá Símanum.

(5) Fjarskiptastofa hóf forskoðun á umræddu öryggisatviki með bréfi dags. 9. desember 2021. Í bréfi stofnunarinnar til félagsins var óskað ítarlegri upplýsinga er varða tildrög öryggisatviksins, áhrif þess á viðskiptavini félagsins sem og um þær úrbætur sem að félagið hugðist fara í til að koma í veg fyrir að sambærileg atvik myndu endurtaka sig. Þá var jafnframt óskað eftir að félagið myndi afhenda stofnuninni gögn sem myndu styðja við svör félagsins. Nánar tiltekið var farið fram á eftirfarandi upplýsingar:

1. *Lýsing á þeirri atburðarás sem átti sér stað þann 12. október sl. sem leiddi til þjónusturofs.*
2. *Lýsing á þeirri atburðarás sem átti sér stað eftir að þjónusturof varð og þar til kerfi voru að fullu endurreist, s.s. upplýsingar um til hvaða aðgerða var gripið eða hvort neyðaráætlun var virkjuð.*
3. *Lýsing á þeim áhrifum sem þjónusturofið hafði á kerfi Símans hf. og viðskiptavini fyrirtækisins, þ.m.t. fjölda notenda, dreifingu og niðritíma þjónustunnar.*
4. *Lýsingu á þeim úrbótum sem Síminn hf. ætlar að gera til að koma í veg fyrir að svipuð atvik endurtaki sig.*

(6) Stofnuninni barst svar frá félaginu með tölvupósti þann 27. desember 2021. Meðfylgjandi tölvupóstinum var frávikaskýrsla (e. Incident Report) frá framleiðandanum [birgir og þjónustuveitandi Símans][13].

[6] Hluti frávikaskýrslu ekki birt opinberlega.
[7] Hluti frávikaskýrslu ekki birt opinberlega.
[8] Hluti frávikaskýrslu ekki birt opinberlega.
[9] Hluti frávikaskýrslu ekki birt opinberlega.
[10] Hluti frávikaskýrslu ekki birt opinberlega.
[11] Hluti frávikaskýrslu ekki birt opinberlega.
[12] Hluti frávikaskýrslu ekki birt opinberlega.
[13] Nafn birgisins og þjónustuveitandans ekki birt opinberlega.

(7) Í svari Símans kemur fram að *„[f]arsímakjarnar Símans eru […][14]. Mannleg mistök urðu við vinnu framleiðanda við uppfærsluna og varð truflun á "live" hlut kerfisins sem orsakaði að svokallaðan […][15], sem er hluti af farsímakjarna Símans, missti samband við aðrar kerfiseiningar. Sem svo olli afgerandi truflunum á talþjónustu yfir 3G og 2G í 32 mínútur."* Er enn fremur vísað til frávikaskýrslu [birgis og þjónustuveitanda Símans][16] fyrir frekari lýsingu á áhrifum.

(8) Þá kemur einnig fram í tölvupósti Símans að áhrif af þessu atviki uppgötvist nánast samstundis. Segir í svarinu að *„[s]érfræðingar Símans átta sig fljótlega á því að bilun tengist […][17] og samhliða hafa samband við teymið sem að vinnur að uppfærslu á óvirka hluta kerfis."* Þá segir jafnframt að breytingastjóri félagsins hafi verið upplýstur og undirbúningur að aðgerðum m.t.t. breytingastjórnunar/neyðaráætlunar undirbúinn. Eins segir að *„[þ]ar sem að mjög skamman tíma tók að endurreisa kerfið var neyðaráætlun ekki virkjuð."* Þá er sett fram í tölvupóstinum tímalína aðgerða hjá félaginu.

(9) Hvað varðar þau áhrif sem að öryggisatvikið hafði þá kemur fram í svari Símans og frávikaskýrslu [birgis og þjónustuveitanda Símans][18] að hluti af farsímakjarna Símans hefði misst samband við aðrar kerfiseiningar sem svo olli afgerandi truflunum á talþjónustu yfir 3G og 2G. Náði truflunin til allt að 150.000 notenda í 32 mínútur. Að auki hafði þessi bilun áhrif á hluta fastlínukerfa Símans þar sem númeraflutningsuppfletting er sameiginleg með farsíma og talsíma í kerfum Símans. Áætlað var að um 50% af fastlínuuppköllum á þessu tímabili hafi einnig orðið fyrir áhrifum og að niðritími hafi verið um 30 mínútur.

(10) Í svari Símans sagði jafnframt að farið hefði verið yfir atvikið og verkferla með framleiðanda, og vísað í frávikaskýrslu frá [birgis og þjónustuveitanda Símans][19] sem fylgdi með svarinu. Eins segir að hvort tveggja atvikinu og eftirfylgni þess sé lokið af hálfu félagsins og [birgis og þjónustuveitanda Símans][20].

(11) Í frávikaskýrslu [birgis og þjónustuveitanda Símans][21] er að finna lýsingu á útfallinu. Í samandreginni lýsingu (e. Executive summary) segir:

> *As a part of the Siminn […][22] upgrade project, due to trooupleshooting 11:30 GMT, [birgir og þjónustuveitandi Símans] by human mistake changed/modified the […][23], when it was commited/saved it was directly replicated and impacted the active […][24], and result was loss of connectivity between the active […][25], but after customer*

[14] Hluti bréfs ekki birt opinberlega.
[15] Hluti bréfs ekki birt opinberlega.
[16] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[17] Hluti tölvupóstsins ekki birt opinberlega
[18] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[19] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[20] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[21] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[22] Hluti bréfs ekki birt opinberlega.
[23] Hluti bréfs ekki birt opinberlega.
[24] Hluti bréfs ekki birt opinberlega.
[25] Hluti bréfs ekki birt opinberlega.

complaints and […][26] degrade observed, Siminn contacted the project main interface […][27] 11:50 GMT and informed about the current situation, immediately after the [birgir og þjónustuveitandi Símans][28] project team changed/rolled back to the correct […][29], and all […][30] was restored 12:02 GMT and confirmed 12:10 GMT.

(12) Eftirfarandi tímalína atburða kemur fram í svari Símans sem og frávikaskýrslu [birgis og þjónustuveitanda Símans][31]:

[…][32]

(13) Í skýrslu [birgis og þjónustuveitanda Símans][33] sagði jafnframt að áhrif hefðu verið eftirfarandi:

[…][34]

Mynd 1: Myndin sýnir lýsingu á áhrifum öryggisatviksins í frávikaskýrslu [birgis og þjónustuveitanda Símans][35], dags. 17. desember 2021, sbr. skjalið „[…][36]“.

(14) Í skýrslu [birgis og þjónustuveitanda Símans][37] sagði einnig að orsök og lagfæring hefði verið eftirfarandi:

[…][38]

Mynd 2: Myndin sýnir lýsingu á orsökum öryggisatviksins og þeirra lagfæringa sem gripið var til í frávikaskýrslu [birgis og þjónustuveitanda Símans], dags. 17. desember 2021, sbr. skjalið „[…][39]“.

(15) Þá kemur fram að til að fyrirbyggja svipuð atvik í framtíðinni hyggist fyrirtækið grípa til eftirfarandi aðgerða:

---

26 Hluti bréfs ekki birt opinberlega.
27 Hluti bréfs ekki birt opinberlega.
28 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
29 Hluti bréfs ekki birt opinberlega.
30 Hluti bréfs ekki birt opinberlega.
31 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
32 Hluti bréfs og frávikaskýrslu ekki birt opinberlega.
33 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
34 Hluti frávikaskýrslu ekki birt opinberlega.
35 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
36 Heitis skjals ekki birt opinberlega.
37 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
38 Hluti frávikaskýrslu ekki birt opinberlega.
39 Heiti skjalsins ekki birt opinberlega.

[…][40]

Mynd 3: Myndin sýnir lýsingu á því hvernig fyrirbyggja skuli svipuð atvik í framtíðinni í frávikaskýrslu [birgir og þjónustuveitandi Símans][41], dags. 17. desember 2021, sbr. skjalið „[…][42]“.

2.2 Niðurstaða forskoðunar

(16) Á grundvelli þeirra upplýsinga og gagna sem að Fjarskiptastofa aflaði í forskoðun sinni komst stofnunin að þeirri niðurstöðu að skoða þyrfti með ítarlegri hætti þá þætti í öryggisskipulagi Símans er varða; áhættumat, breytingastjórnun og neyðaráætlun félagsins. Markmið stjórnsýsluskoðunarinnar var að ganga úr skugga um hvort undirbúningur og framkvæmd breytingarinnar sem olli öryggisatvikinu sem og viðbrögð við því hafi verið í samræmi við þær lagakröfur sem á félaginu hvíla skv. þágildandi lögum um fjarskipti nr. 81/2003, sbr. einnig ákvæði reglna 1221/2007 og 1222/2007, sbr. ákvæði I til bráðabirgða í lögum nr. 70/2022, um fjarskipti.

(17) Hvað varðar neyðaráætlun þá byggir þessi niðurstaða stofnunarinnar m.a. á því að í svörum Símans kom fram að tæknimenn hefðu strax orðið varir við bilunina og haft samband við [birgi og þjónustuveitanda Símans][43], en í skýrslu [birgis og þjónustuveitanda Símans][44] kom fram að ekki hafi orðið vart við bilunina fyrr en viðskiptavinir höfðu samband við Símann og eftir greiningu í KPI mælingum. Í framhaldinu hafði Síminn, klukkan 11:50, samband við […][45] sem skráði atvik […][46] klukkan 11:53. Í framhaldinu keyrði [birgis og þjónustuveitanda Símans][47] áður gerðar breytingar til baka og eðlileg virkni komst á klukkan 12:02.

(18) Af framangreindu er ljóst að frá því að atvik er skráð hjá [birgi og þjónustuveitanda Símans][48] líða níu mínútur þar til þjónusta var komin aftur á, en heildartími öryggisatburðarins var 32 mínútur. Þannig líða um 20 mínútur frá því bilun á sér stað þar til Síminn bregst við með því að hafa samband til verkefnateymi (e. project team) […][49], sbr. frávikaskýrslu [birgis og þjónustuveitanda Símans][50].

(19) Í þeim svörum félagsins segir einnig að breytingastjóri Símans hefði verið upplýstur og undirbúningur að aðgerðum m.t.t. til breytingastjórnunar og neyðaráætlunar undirbúin, en þar sem að mjög skamman tíma hefði tekið að endurreisa kerfið hafi neyðaráætlun ekki verið virkjuð, en síðar kom þó fram í svörum Símans að neyðaráætlun hafi í raun verið virkjuð en nokkuð eftir að atvikið átti sér stað. Með hliðsjón af þeim tíma sem leið frá því bilun kom upp og þar til brugðist var við, vöknuðu upp spurningar hjá Fjarskiptastofu um hvernig vöktun

[40] Hluti frávikaskýrslu ekki birt opinberlega.
[41] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[42] Heiti skjalsins ekki birt opinberlega.
[43] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[44] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[45] Hluti ákvörðunar ekki birtur opinberlega, þ.m.t. nafn birgis og þjónustuveitanda Símans.
[46] Hluti ákvörðunar ekki birtur opinberlega.
[47] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[48] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[49] Hluti ákvörðunar ekki birtur opinberlega, þ.m.t. nafn birgis og þjónustuveitanda Símans.
[50] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

Símans á kerfum sínum væri háttað, enda hafi ekki orðið vart við bilunina fyrr en viðskiptavinir höfðu samband við Símann og eftir greiningu í KPI mælingum, sbr. frávikaskýrsla [birgis og þjónustuveitanda Símans][51].

(20) Þegar kemur að breytingarstjórnun hjá félaginu þá virðist sem svo, af svörum [birgis og þjónustuveitanda Símans][52] að dæma, að skort hafi á þekkingu þeirra starfsmanna sem komu að uppfærslunni. Jafnframt er talað um það í skýrslunni að allan aðgang aðila að kerfum þurfi að samþykkja en slíkt vekur upp spurningar um hvernig staðið er að samþykki og veitingu aðgangsheimilda í kjarnakerfi farsímaþjónustu hjá Símanum.

(21) Jafnframt var talað um það í skýrslu [birgis og þjónustuveitanda Símans][53] að skilja þurfi á milli […][54] verði bætt og að samskipti aðila verði stöðug á meðan breytingar eiga sér stað og að sett verði upp prófunarumhverfi.

(22) Í frávikaskýrslu þeirri sem Fjarskiptastofu barst frá atvikastjórnun Símans þann 19. október 2021 kemur fram að venjan sé sú hjá Símanum að allar breytingar sem gætu haft áhrif á neytendur skuli gerðar að nóttu til. Talað er um að halda sig við þá venju í framtíðinni. Þá kemur heldur ekki fram í svörum Símans í tölvupósti frá 27. desember 2021 hvernig staðið var að breytingastjórnun í tengslum við uppfærslu [birgis og þjónustuveitanda Símans][55] á kerfunum, eða af hverju breytingar voru gerðar og keyrðar í raunumhverfi, eins og ætla mátti m.t.t. eðlis öryggisatviksins. Ekkert kemur þar heldur fram um gildandi viðmið um hvenær heimilt er að gera breytingar á kerfum.

(23) Með hliðsjón af þeirri framkvæmd sem virtist hafa verið viðhöfð vöknuðu upp spurningar hjá Fjarskiptastofu um það hvernig Síminn stæði almennt að þáttum sem varða stjórnunarkerfi fyrirtækisins um upplýsingaöryggi. Var því óskað eftir upplýsingum er varða framkvæmd áhættumats hjá félaginu.

(24) Með hliðsjón af framangreindu, eðli öryggisatviksins og upplýsingum frá Símanum boðaði Fjarskiptastofa stjórnsýslurannsókn þann 6. maí 2022 til að skoða afmarkaða þætti sem varða stjórnkerfi upplýsingaöryggis hjá Símanum. Um er að ræða þætti sem varða; áhættumat, breytingastjórnun og neyðaráætlun til að ganga úr skugga um hvort undirbúningur, framkvæmd og viðbrögð við atviki því sem varð 12. október 2021 hafi verið í samræmi við þær lagakröfur sem á félaginu hvíla.

III. Lagaumhverfi

(25) Fjarskiptastofa er sú stofnun sem með lögum hefur verið falið að annast stjórnsýslu og eftirlit með framkvæmd fjarskipta- og netöryggismála, sbr. 2. gr. laga nr. 75/2021, um Fjarskiptastofu. Þannig skal stofnunin annast eftirlit á framkvæmd laga um fjarskipti. Er markmið með starfsemi Fjarskiptastofu m.a. að stuðla að skilvirkum og öruggum fjarskiptum

[51] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[52] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[53] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[54] Hluti ákvörðunar ekki birt opinberlega.
[55] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

og stuðla að öryggi almennings, fyrirtækja og samfélagsins alls á sviði fjarskipta og netöryggis, sbr. 1. og 2. mgr. 3. gr. laganna.

(26) Þegar öryggisatvikið átti sér stað voru í gildi fjarskiptalög nr. 81/2003 og verður því atvikið metið út frá kröfum þeirra laga. Í 47. gr. þágildandi fjarskiptalaga var fjallað um öryggi og þagnarskyldu í fjarskiptum. Ákvæði 47. gr. var ætlað að gegna lykilhlutverki þegar kemur að leynd fjarskipta, til verndar friðhelgi einkalífs áskrifenda og er mikilvægur þáttur í öryggi fjarskiptaþjónustu. Sá hluti ákvæðisins er varðar kröfur um vernd upplýsinga er að finna í 1. og 2. mgr. ákvæðisins og kom að mestu leyti inn í fjarskiptalög með lögum, nr. 39/2007, um breytingu á lögum um fjarskipti nr. 81/2003. Voru með þeirri lagabreytingu lagðar skyldur á fjarskiptafyrirtæki um að verja upplýsingar sem fara um fjarskiptanet þeirra og skjalfestingu á skipulagi upplýsingaöryggis. Var hér lögfest inntak upplýsingaöryggis, þ.e. að tryggja skuli leynd upplýsinga, lögmæti aðgangs að þeim og réttleika.

(27) Málsgreinarnar eru svohljóðandi:

> *Fjarskiptafyrirtæki sem veita almenna fjarskiptaþjónustu skulu gera viðeigandi ráðstafanir til þess að tryggja öryggi þjónustunnar í samráði við rekstraraðila fjarskiptaneta ef við á. Verja skal upplýsingar sem fara um fjarskiptanet gegn því að þær glatist, skemmist eða breytist fyrir slysni eða að óviðkomandi fái aðgang að þeim. Ef sérstök hætta er á að leynd fjarskipta á tilteknu neti verði rofin skal þjónustuveitandinn upplýsa áskrifendur um hættuna.*
>
> *Fjarskiptafyrirtæki skulu skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, gera áhættumat og ákveða öryggisráðstafanir á grundvelli þess. [Fjarskiptastofa] setur reglur um vernd upplýsinga í almennum fjarskiptanetum þar sem nánar er mælt fyrir um þær kröfur sem gerðar eru til skipulags upplýsingaöryggis. Skulu reglurnar m.a. kveða á um:*
>
> *a. hvernig skjalfesta skuli skipulag upplýsingaöryggis,*
> *b. hlítingu við tiltekna staðla,*
> *c. framkvæmd innra eftirlits,*
> *d. helstu öryggisráðstafanir sem viðhafa skal,*
> *e. tilkynningar vegna öryggisrofs,*
> *f. eftirlitsúrræði [Fjarskiptastofu].*

(28) Þannig gerir 47. gr. laganna þá kröfu til fjarskiptafyrirtækja að skjalfesta skipulag upplýsingaöryggis með því að setja sér öryggisstefnu, gera áhættumat og ákveða öryggisráðstafanir á grundvelli þess, sbr. 2. mgr. ákvæðisins. Þá skal fjarskiptafyrirtæki jafnframt gera sérstakar ráðstafanir til að tryggja samfelldan og órofinn rekstur almennra fjarskiptaneta, sbr. 3. mgr. ákvæðisins. Í sömu málsgreinum er mælt fyrir um að Fjarskiptastofa setji sérstakar reglur um vernd upplýsinga og virkni almennra fjarskiptaneta. Í þessu skyni, og með heimild í b-lið 9. gr. laga nr. 39/2007, hefur stofnunin sett reglur nr. 1221/2007, um vernd upplýsinga í almennum fjarskiptanetum og reglur nr. 1222/2007, um virkni almennra fjarskiptaneta, en þar er nánar kveðið á um hvernig virkni almennra fjarskiptaneta skuli tryggð með sem bestum hætti. Þar er kveðið á um þær lágmarksráðstafanir sem taldar eru

nauðsynlegar, eftir því sem við á, að fjarskiptafyrirtækin viðhafi, til að tryggja samfelldan rekstur almennra fjarskiptaneta sinna og vernd þeirra. Þá er sérstaklega tilgreint að þær kröfur sem ekki koma beint fram í reglunum skuli fyrirtækin sjálf bera kennsl á með skipulegu áhættumati og viðhafa aðgerðir til að stýra og stjórna fjarskiptanetum með tilliti til áhættu, sbr. 4. gr. áðurnefndra reglna nr. 1222/2007. Er fjarskiptafyrirtækjum þannig gert að nýta sér áhrifagreiningu og áhættumat til að draga úr öllum stærri veikleikum og veilum í innviðum sínum.

(29) Framangreindar skyldur fjarskiptafyrirtækja eru nánar útfærðar í 7. gr. áðurnefndra reglna Fjarskiptastofu nr. 1221/2007. Í 1. tölul. ákvæðisins er kveðið á um að fjarskiptafyrirtæki setji sér skriflega öryggisstefnu. Í 2. tölul. er fjallað um gerð skriflegs áhættumats með það að markmiði að skapa forsendur fyrir vali á öryggisráðstöfunum og skal það endurskoðað reglulega. Þá skal fjarskiptafyrirtæki samkvæmt 3. tölul. greinarinnar gera ákveðnar öryggisráðstafanir og setja fram skriflegar lýsingar á þeim. Þannig skal fjarskiptafyrirtækið m.a. skilgreina hvaða öryggisráðstöfunum skuli beitt, hvernig þær verði útfærðar sem og taka fram hvernig brugðist verði við áföllum í rekstri fjarskiptaneta. Ákvæðið er svohljóðandi:

> *Fjarskiptafyrirtæki skulu útbúa og viðhalda skjalfestri lýsingu á stjórnkerfi sem tryggir upplýsingaöryggi í fjarskiptaþjónustu og fjarskiptanetum. Þetta stjórnkerfi upplýsingaöryggis skal að lágmarki felast í eftirtöldu:*
>
> 1. *Fjarskiptafyrirtæki skal setja sér skriflega öryggisstefnu. Í henni skal m.a. koma fram almenn lýsing á afstöðu æðsta stjórnanda fjarskiptafyrirtækis til öryggismála. Í stefnunni skulu koma fram markmið og meginreglur upplýsingaöryggis samkvæmt rekstrarstefnu og rekstrarmarkmiðum. Stefnan skal kynnt öllum starfsmönnum fjarskiptafyrirtækisins sem hafa með fjarskiptarekstur að gera. Við mótun öryggisstefnu skal taka mið af því hvaða upplýsingar skuli vernda, hvernig skuli vernda þær, þeirri aðferð sem viðhöfð verður við vinnslu þeirra og hver beri ábyrgð á öryggi þeirra. Skal öryggisstefnan birt starfsmönnum.*
>
> 2. *Fjarskiptafyrirtæki skal skilgreina aðferðarfræði áhættumats um upplýsingaöryggi og henni fylgt eftir með skriflegu áhættumati um upplýsingaöryggi sem tengist fjarskiptanetum og fjarskiptaþjónustu. Áhættumat skal bera kennsl á áhættuþætti, umfang þeirra og forgangsraða þeim miðað við ásættanlega áhættu og þau markmið sem skipta máli fyrir fyrirtækið. Áhættumat skal skilgreina eignir og gera á þeim einfalt mat og mat á þeim áhrifum sem myndast af völdum rofs á leynd, réttleika og tiltækileika. Miklir veikleikar og ógnir eru skilgreind fyrir eignirnar, ásamt mati á líkindum þeirra. Áhættan fyrir hvert atriði er reiknuð út og hún borin saman við fyrir fram gerðan mælikvarða um ásættanlegt áhættustig um öryggi upplýsinga, órofinn rekstur og þjónustustig. Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum og skal það endurskoðað reglulega.*
>
> 3. *Fjarskiptafyrirtæki skulu setja sér verklagsreglur um örugga meðferð upplýsinga og eyðingu þeirra. Gerðar skulu öryggisráðstafanir og settar fram skriflegar lýsingar á þeim. Tilgreina skal hvaða öryggisráðstöfunum verði beitt og hvernig*

þær verði útfærðar, þ. á m. við hönnun, þróun, rekstur, prófun og viðhald hvers kerfis. Þá skal og tekið fram hvernig brugðist verði við áföllum í rekstri fjarskipta-neta og fjarskiptaþjónustu. Öryggisráðstafanir skal endurskoða reglulega. Skriflegar leiðbeiningar skulu vera til staðar fyrir einstaka ferla sem nauðsynlegir eru fyrir upplýsingaöryggi fjarskiptaneta og fjarskiptaþjónustu. Fjarskiptafyrirtækið skal sjá til þess að ákvæðum stefnunnar um upplýsingaöryggi sé framfylgt, líka þegar verktakar vinna fyrir fyrirtækið. Fjarskiptafyrirtækið skal sjá til þess að starfsmenn þess framfylgi stefnunni um upplýsingaöryggi.

(30) Í II. kafla reglna 1222/2007 er að finna almennar kröfur og leiðbeiningar en þar segir í 4. gr. að:

Í reglum þessum koma fram kröfur til fjarskiptafyrirtækja um að tryggja virkni og öryggi fjarskiptaneta, þ.e. hinna eiginlegu fjarskiptaneta svo og upplýsingakerfa sem þau styðjast við og tengjast, svo sem aðgangs- og reikningakerfi, hér eftir nefnt fjarskiptanet. Þær kröfur sem ekki koma beint fram í reglum þessum, skulu fjarskiptafyrirtæki sjálf bera kennsl á með skipulegu áhættumati og viðhafa aðgerðir til að stýra og stjórna fjarskiptanetum með tilliti til áhættu. Til hliðsjónar má styðjast við staðlana ISO/IEC 27001 (Stjórnkerfi upplýsingaöryggis) og ISO/IEC 17799 (Starfsvenjur fyrir stjórnun upplýsingaöryggis). Fara skal eftir nýjustu útgáfu staðlanna á hverjum tíma. Staðlana má ennfremur nota sem leiðbeiningar um ráðstafanir sem innleiða má til að uppfylla kröfur reglnanna.

(31) Í 5. gr. er svo fjallað um hlítingu við staðla, þar segir:

Nánari tæknileg útfærsla á framkvæmd atriða í þessum reglum er skilgreind í ITU stöðlum (International Telecommunication Union), þýddum og útgefnum af Staðlaráði Íslands. Ef þýðingar eru ekki til staðar, er stuðst við enska útgáfu ITU staðlanna, svo framarlega sem þeir eru til. Annars er stuðst við leiðbeiningarit ITU, ISO eða IEC staðla, eða önnur tiltæk almennt viðurkennd gögn, t.d. útgefin af IEFT. Sama gildir um atriði utan þessara reglna.

(32) Sambærilegt ákvæði er að finna í 2. gr. reglna nr. 1221/2007, þar sem fram kemur að „[t]*il hliðsjónar má styðjast við staðlana ISO/IEC 27001 (Stjórnkerfi upplýsingaöryggis) og ISO/IEC 17799 (Starfsvenjur fyrir stjórnun upplýsingaöryggis). Fara skal eftir nýjustu útgáfu staðlanna á hverjum tíma. Staðlana má ennfremur nota sem leiðbeiningar um ráðstafanir sem innleiða má til að uppfylla kröfur reglnanna.*“.

(33) Þá er einnig er fjallað um áhættugreiningu og áhættumat í 7. gr. reglna nr. 1222/2007, um virkni almennra fjarskiptaneta. Þar segir:

Fjarskiptafyrirtæki skulu nýta sér áhrifagreiningu og áhættumat til að draga úr öllum stærri veikleikum og veilum í innviðum sínum.

Í áhrifagreiningu eru dregin fram þau atvik sem geta valdið þjónusturofi, m.a. vegna bilunar, óhappa eða annarra atvika sem ógna öryggi þeirra, t.d. af völdum náttúru-hamfara, mannskæðra farsótta, slysa, straumleysis, bilunar í búnaði, innbrota, skemmdarverka o.s.frv.

Í áhættumati skal meta líkindi þess að atvikin eigi sér stað og hugsanleg áhrif atvikanna að teknu tilliti til veikleika í fjarskiptarekstri og í fjarskiptanetum.

Í áhættumati skal greina sérstaklega alla mikilvæga innviði. Lýsa skal notkun á mikil-vægu innviðunum og samtengingum þeirra við aðra hluta fjarskiptanetsins og við önnur fjarskiptanet. Enn fremur skal lýsa hvernig öryggi mikilvægu innviðanna er tryggt á besta mögulega hátt, þ.m.t. vernd gegn straumrofi, upplýsinga- og vöktunarkerfi, aukaleiðir, viðbragðsbúnaður, þjónustusamningar, vernd gegn öryggisatvikum, raunlæg vernd og hvernig er staðið að öryggisafritun.

Við gerð áhættumats skal fylgja að öðru leyti þeim leiðbeiningum sem fram koma í 7. gr. reglna [Fjarskiptastofu] nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum.

(34) Þegar áhættumat liggur fyrir, þ.m.t. greining á mikilvægum innviðum fjarskiptanetsins, ber fjarskiptafyrirtækjum einnig að setja sér neyðaráætlun um ráðstafanir til að tryggja samfelldan og órofinn rekstur, m.a. um hvernig skuli standa að því að endurræsa óvirk fjarskiptanet og mögulega endurheimta upplýsingar sem kunna að hafa misfarist og skemmst en í 8. gr. reglna nr. 1222/2007 er fjallað um kröfur um neyðaráætlun, en þar segir:

Gerðar skulu ráðstafanir til að tryggja samfelldan og órofinn rekstur almennra fjar-skiptaneta og fjarskiptaþjónustu. Í því skyni skulu fjarskiptafyrirtæki setja sér skrif-lega neyðaráætlun, sem byggir á niðurstöðum áhættumats. Í samræmi við það skal lýsa áætlun um ráðstafanir til að endurræsa óvirk fjarskiptanet og mögulega endur-heimta upplýsingar sem kunna að hafa misfarist eða skemmst. Áætlunina skal prófa reglulega til að tryggja virkni hennar.

(35) Í ákvæðinu eru jafnframt sett fram hvað skal að lágmarki koma fram í neyðaráætluninni, sbr. tl. 1-5:

1. *Lýsing á skipulagi og ábyrgð viðbragðshópa.*
2. *Lýsing á viðhaldi handbóka fyrir daglegan rekstur búnaðar.*
3. *Verkferlar fyrir gangsetningu áfallalausna.*
4. *Skilgreining á hámarkstíma rekstrarstöðvunar áður en gripið er til áætlunarinnar.*
5. *Upplýsingar um helstu tengiliði birgja og þjónustuaðila.*

(36) Þá er í 9. gr. áðurnefndra reglna nr. 1222/2007, sbr. einnig 8. gr. reglna nr. 1221/2007, fjallað um innra eftirlit. Þar segir að viðhafa skuli innra eftirlit til að tryggja virkni

neyðaráætlunar. Innra eftirlit skal framkvæma kerfisbundið samkvæmt fyrir fram skilgreindri aðferð. Þá segir einnig:

Verkferlum sem tryggja samfelldan rekstur skal haldið við og skulu þeir endurspegla sem næst raunverulegar rekstrarkröfur hverju sinni. Tíðni og umfang eftirlitsins skal ákveðið með hliðsjón af skilgreindri áhættu og mikilvægi þeirra fjarskiptaneta sem um er að ræða, tækni sem notuð er til að tryggja öryggi þeirra og kostnaði af framkvæmd eftirlitsins. Það skal þó framkvæmt eigi sjaldnar en árlega. Eftirlit með virkni neyðaráætlunar skal vera hluti af reglulegu innra eftirliti.

(37) Þá er í 20. gr. reglnanna settar kröfur um viðhald fjarskiptaneta. Í ákvæðinu segir:

Á meðan fjarskiptanet eru í notkun, skal fjarskiptafyrirtækið viðhalda rekstri þeirra og fjarskiptaþjónustunnar og reisa þau skjótt við til fullrar virkni eftir bilun.

Tryggja skal að til staðar séu afrit af síðustu stillingum búnaðar sem nauðsynlegar eru til að reisa við fjarskiptanet og tengd kerfi. Geyma skal afritunargögnin á öruggum stað.

Strax og vart verður við að búnaður valdi truflunum á fjarskiptastarfseminni, skal gera ráðstafanir til að reisa búnaðinn við til fyrra ástands eða aftengja hann frá fjarskiptanetinu ef svo ber undir.

Eftir því sem við á skulu fjarskiptafyrirtæki hafa nægan varabúnað og önnur úrræði til að viðhalda samfelldum rekstri.

(38) Í 21. gr. reglna nr. 1222/2007 er fjallað um fyrirbyggjandi viðhald, en þar segir að fjarskiptafyrirtæki skuli framkvæma fyrirbyggjandi viðhald búnaðar í samræmi við fyrir fram gerða áætlun, til að minnka líkindi á bilun í búnaði.

(39) Í 23. gr. reglna nr. 1222/2007, um virkni almennra fjarskiptaneta er svo fjallað um breytingar í almennum fjarskiptanetum, en þar segir:

Verkferlar sem fjalla um breytingar skulu taka til allra breytinga sem geta haft áhrif á fjarskiptanetin og skulu tryggja viðeigandi formlega meðhöndlun breytinga ásamt skjalfestingu þeirra. Verkferlarnir skulu hafa í för með sér traustan, skipulegan og fyrirsjáanlegan rekstur fjarskiptaneta.

Breytingar skal framkvæma þannig að þær trufli sem minnst fjarskiptaþjónustu fjarskiptafyrirtækisins og annarra fjarskiptafyrirtækja.

Ef breyting hefur óhjákvæmilega áhrif á fjarskiptanet og fjarskiptaþjónustu annarra fjarskiptafyrirtækja, skal vera samvinna milli aðila um fyrirkomulag breytinganna til að minnka truflanir.

(40) Í 12. gr. reglna nr. 1221/2007 er kveðið á um skipulags- og tæknilegar ráðstafanir til að verja almenn fjarskiptanet, en þar segir:

Fjarskiptafyrirtæki skulu viðhafa nauðsynlegar tæknilegar og skipulagslegar ráðstafanir til að verja almenn fjarskiptanet sín. Skulu fjarskiptafyrirtæki m.a. gera eftirfarandi ráðstafanir eftir því sem við á:

1. *Stýringar fjarskiptabúnaðar skulu vera varðar gegn óheimilum aðgangi að skilaboðum og auðkennum í flutningi, svo sem með dulkóðun eða lokuðum stýrinetum.*
2. *Nota aðgangsheimildir, aðgangsstýringu og óhrekjanleika.*
3. *Staðfesta skal að óskir um breytingu á fjarskiptaþjónustu komi frá áskrifanda hennar, eða séu með samþykki hans.*
4. *Tryggja óhrekjanleika aðgerða.*
5. *Tryggja rekjanleika uppflettinga og vinnsluaðgerða.*
6. *Takmarka aðgang starfsmanna að upplýsingum við þær sem eru þeim nauðsynlegar til að þeir geti sinnt starfi sínu, og við þann tíma sem nauðsynlegur er.*
7. *Upplýsingaöflun vegna afgreiðslu og reikningagerðar, skal aðskilja frá öflun upplýsinga um fjarskiptaumferð sem nýtast kann í þágu rannsókna opinberra mála og almannaöryggis, t.d. innihald fjarskipta.*
8. *Viðhalda órofinni slóð sönnunargagna sem nýst gætu vegna öryggisatburða. Skilgreina búnað og vinnslu fyrirfram á þann hátt að sem flest mikilvæg þess háttar tilvik komi með skýrum hætti fram í eftirlitskerfum.*
9. *Halda skrá um aðgangsheimildir og aðgangsréttindi og yfirfara reglulega. Skal fjarskiptabúnaður vera stilltur til samræmis við þá skráningu.*
10. *Viðhafa skal viðeigandi ráðstafanir til að tryggja öryggi upplýsinga í boðskiptum endanna á milli við eftirtaldar aðstæður:*
    a. *Starfsmenn vinna í fjarvinnslu við viðkvæm fjarskiptakerfi.*
    b. *Fjarskiptafyrirtæki veita viðskiptavinum sínum sérstakt fjarvinnsluaðgengi að kerfum viðskiptavinarins, með stýringu og viðkomu í kerfum fjarskiptafyrirtækisins, svo sem aðgengi að pósthúsum eða gagnageymslum fyrirtækja frá farsíma.*

(41) Í 13. gr. reglna nr. 1221/2007 er svo fjallað um útvistun reksturs fjarskiptaneta, en þar segir:

Fjarskiptafyrirtæki er heimilt að semja við þriðja aðila um að annast, í heild eða að hluta, rekstur fjarskiptanets. Stjórnunarlegri ábyrgð og áhættustýringu verður þó ekki útvistað. Skilyrði slíks samnings er þó að fjarskiptafyrirtæki hafi sannreynt að umræddur aðili hafi sett sér öryggisstefnu og geti framkvæmt nauðsynlegar öryggisráðstafanir samkvæmt reglum þessum ásamt innra eftirliti. Gerður skal skriflegur samningur til að tryggja þetta. Samningurinn skal m.a.:

1. *Kveða á um skyldu vistunaraðila að starfa í samræmi við fyrirmæli fjarskiptafyrirtækis og ákvæði reglna þessara.*

2. *Innihalda lýsingu á þeirri þjónustu sem inna skal af hendi og tiltaka það þjónustustig sem stefnt er að. Enn fremur þær ráðstafanir sem gripið skal til ef þjónustan uppfyllir ekki þau ákvæði.*
3. *Hafa ákvæði um þagnarskyldu og með honum skal tryggt að farið sé að ákvæðum fjarskiptalaga þar að lútandi.*
4. *Tryggja að fjarskiptafyrirtækið eigi rétt til eftirlits með þeirri starfsemi sem samningurinn tekur til.*
5. *Tryggja aðgang [Fjarskiptastofu] að upplýsingum frá vistunaraðila og að stofnunin geti í þágu eftirlits framkvæmt athuganir á starfsstöð hans.*

IV. Stjórnsýsluskoðun Fjarskiptastofu

4.1 Afmörkun stjórnsýsluskoðunar og aðildar

(42) Líkt og að framan greinir beindist stjórnsýsluskoðun Fjarskiptastofu á umræddu öryggisatviki að þremur atriðum, þ.e. áhættumati, breytingarstjórnun og neyðaráætlun félagsins. Þess skal getið að í tengslum við breytingarstjórnun var skoðuðu hlítni Símans við reglur um útvistun reksturs fjarskiptaneta og notkunar á varabúnaði og annarra úrræði til að viðhalda samfeldum rekstri fjarskiptaneta, og í tengslum við neyðaráætlun var skoðuð hlítni félagsins við reglur um innra eftirlit.

(43) Stjórnsýsluskoðun Fjarskiptastofu beindist að skipulagi upplýsingaöryggis hjá Símanum, þ.e. hvort að framkvæmd þess sé í samræmi við þær kröfur sem kveðið var á um í þágildandi fjarskiptalögum, og gildandi reglum nr. 1221/2007 og 1222/2007 á þeim tíma sem öryggisatvikið átti sér stað. Ljóst er að Síminn hefur gert þjónustusamning við [birgi og þjónustuveitanda Símans][56], sem er framleiðandi þess búnaðar sem félagið notar í fjarskiptaneti sínu, sem nær til breytinga í kerfum félagsins. Slík útvistun leiðir þó ekki til þess að Síminn sé ekki ábyrgur fyrir framkvæmd öryggismála og rekstri fjarskiptanets síns, sbr. 13. gr. reglna nr. 1221/2007.

(44) Upplýsingaöflun Fjarskiptastofu við stjórnsýsluskoðun þessa beindist að Símanum og afhenti félagið umrædd gögn sem sín eigin. Þannig eru þau gögn sem eiga uppruna sinn hjá [birgi og þjónustuveitanda Símans][57] gögn Símans í máli þessu og á [birgir og þjónustuveitandi Símans][58] ekki aðild að máli þessu.

4.2 Gagnabeiðni Fjarskiptastofu

(45) Með bréfi Fjarskiptastofu, dags. 6. maí 2022, fór stofnunin fram á upplýsingar um umrætt öryggisatvik. Með hliðsjón af alvarleika öryggisatviksins vöknuðu upp spurningar hjá stofnuninni um hvernig staðið hafi verið að **áhættumati** umræddrar uppfærslu sem og hvernig

[56] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[57] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[58] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

tengd kerfi og aðstaða er almennt metin í áhættumati Símans með hliðsjón af 7. gr. reglna nr. 1222/2007 og 2. tl. 7. gr. reglna nr. 1221/2007. Var óskað eftirfarandi gagna:

1. *Afrit af verklagsreglu um áhættumat (meðferð um upplýsingaöryggisáhættu).*
2. *Afrit af skriflegu áhættumati upplýsingaöryggis.*
3. *Staðfest áhættumat (breytingabeiðni) á þeim breytingum sem verið var að vinna þegar útfallið varð 12. október síðastliðinn.*

(46) Með hliðsjón af því að **neyðaráætlun** var ekki virkjuð strax og atvik átti sér stað vöknuðu upp spurningar um vöktun og virkjun neyðaráætlunar. Í 8. gr. reglna nr. 1222/2007 er gerð krafa um skriflega neyðaráætlun sem byggir á niðurstöðu áhættumats og reglulegar prófanir á neyðaráætlun og í 9. gr. reglna nr. 1222/2007, er fjallað um innra eftirlit til að tryggja virkni neyðaráætlunar. Var farið fram á að Síminn afhendi eftirfarandi gögn:

1. *Afrit af skriflegri neyðaráætlun fyrirtækisins og tengd gögn sem sýna fram á virkni þeirra lágmarkskrafna (tl. 1-5. í 8. gr. reglna nr. 1222/2007) sem koma eiga fram í neyðaráætlun.*
2. *Lýsingu á ferlum (verklagi) um vöktun kerfa sem til staðar eru til að tryggja samfelldan rekstur.*
3. *Afrit af síðustu þremur prófunum á neyðaráætlun og niðurstöðum þeirra.*
4. *Afrit af gildandi áætlun innra eftirlits.*
5. *Niðurstöðum og staðfestum skoðunum innra eftirlits á neyðaráætlun síðastliðin þrjú ár.*

(47) Hvað varðar **breytingastjórnun** vöknuðu upp spurningar um hvort gildandi verkferlar séu í samræmi við 23. gr. reglna 1222/2007. Var óskað eftir að Síminn afhendi eftirfarandi gögn:

1. *Afrit af skjalfestum verkferlum við breytingastjórnun.*
2. *Lista yfir breytingar sem gerðar hafa verið á fjarskiptakerfum síðastliðna 12 mánuði.*
3. *Afrit af breytingarbeiðni vegna þeirra breytinga sem verið var að vinna þegar útfallið varð 12. október síðastliðinn.*

(48) Auk framangreindra gagna óskaði Fjarskiptastofa eftir því að fá svör við eftirfarandi spurningum:

1. *Hverjar eru ástæður þess að […][59] upplýsti ekki strax um bilun í kjarnakerfi farsímaþjónustu Símans?*
2. *Hverjar eru ástæður þess að neyðaráætlun var ekki virkjuð um leið og atvikið varð?*
3. *Hvernig og hvenær var neyðaráætlun virkjuð?*
4. *Í fyrri svörum frá félaginu kom fram að óheimilt er að gera breytingar á kjarnakerfum á dagtíma.*

[59] Hluti bréfs ekki birtur opinberlega.

a. *Hverjar eru ástæður þess að breytingar voru gerðar beint í kjarnakerfum fjarskiptaþjónustu á dagtíma?*
b. *Hvernig var staðið að samþykki Símans á breytingunum?*
c. *Með hvaða hætti eru kröfur um upplýsingaöryggi, m.a. breytingarstjórnun miðlað til [birgis og þjónustuveitanda Símans][60] (þriðja aðila)?*
5. *Hvernig var aðgangsheimildum [birgis og þjónustuveitanda Símans][61] háttað inn í kerfi Símans?*
a. *Var aðgangur veittur til einstaklinga eða er um hópaðgang að ræða?*
b. *Ef um tímabundinn aðgang var að ræða, hvernig var hann þá skipulagður?*
c. *Hver voru tímamörk og breytingarheimildir á aðgangi [birgis og þjónustuveitanda Símans][62] háttað á þeim tíma sem atvikið varð?*
6. *Eru fyrirhugaðar breytingar á kjarnakerfum félagsins prófaðar áður en þær eru keyrðar í raunumhverfi?*
7. *Eru gerðar áætlanir um prófanir á kjarnakerfum félagsins?*

(49) Með bréfi, dags. 5. janúar 2023, var Símanum send boðun ákvörðunar vegna umrædds öryggisatviks. Stofnuninni bárust andmæli frá Símanum 15. febrúar 2023. Eftir yfirferð Fjarskiptastofu á svörum Símans var það mat stofnunarinnar að komið hafi fram nýjar upplýsingar sem lágu ekki fyrir. Óskaði stofnunin því eftir frekari upplýsingum og gögnum með bréfi, dags. 10. ágúst 2023, til að tryggja að málið væri nægilega upplýst. Lutu spurningar Fjarskiptastofu m.a. að atriðum í tengslum við rannsókn stofnunarinnar á breytingarstjórnun, varðandi hlítni Símans við reglur um útvistun rekstur fjarskiptaneta, sbr. 13. gr. reglna nr. 1221/2007 og notkunar á varabúnaði og annarra úrræði til að viðhalda samfeldum rekstri fjarskiptaneta, sbr. 20. gr. reglna nr. 1222/2007, og einnig að atriðum í tengslum við rannsókn á neyðaráætlunar varðandi innra eftirlit, sbr. 9. gr. reglna nr. 1222/2007.

4.3 Gögn og upplýsingar frá Símanum

(50) Fjarskiptastofu bárust svör og gögn frá Símanum vegna fyrri gagnabeiðni stofnunarinnar þann 24. maí 2022. Vegna síðari gagnabeiðninnar, dags. 10. ágúst 2023, bárust svör og gögn frá Símanum þann 11. september 2023. Um er að ræða nokkuð magn gagna sem Fjarskiptastofa hefur skoðað en ekki er ástæða að gera grein fyrir þeim í öllum atriðum í ákvörðun þessari. Verður hins vegar vísað til þeirra eftir því sem við á í forsendum ákvörðunarinnar.

4.4 Forsendur niðurstöðu stjórnsýsluskoðunar

4.4.1 Áhættumat

(51) Í gagnabeiðni Fjarskiptastofu frá 6. maí 2022 var beðið um afrit af verklagsreglu um áhættumat og afhenti Síminn 24. maí 2022 í skjalinu: „Svarbréf til Fjarskiptastofu.pdf“ afrit af hluta verklagsreglna Símans um áhættumat ([…][63]) þar sem farið var yfir framkvæmd áhættumats. Einnig var í framangreindri gagnabeiðni beðið um afrit af skriflegu áhættumati upplýsingaöryggis svo leggja mætti mat á virkni áhættumats. Síminn afhenti svo

[60] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[61] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[62] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[63] Heiti verklagsreglna ekki birt opinberlega.

Fjarskiptastofu skjalið „[…][64]“ og skjalið „[…][65]“ í samræmi við síðari gagnabeiðni stofnunarinnar þann 11. september 2023.

(52) Í framangreindum skjölum kemur fram skilgreind aðferðarfræði áhættumats hjá Símanum og er þar ferli áhættumats hjá félaginu ítarlega lýst. Í svörum Símans segir svo að […][66].

(53) Í gagnabeiðni Fjarskiptastofu, dags. 6. maí 2022, var einnig óskað eftir að Síminn afhenti staðfest áhættumat vegna þeirra breytinga sem verið var að vinna þegar útfallið varð 12. október 2021. Sem svar við gagnabeiðninni afhenti Síminn skjalið: „Svarbréf til Fjarskiptastofu.pdf“ sem innihélt m.a. skjáskot af breytingabeiðni úr […][67] vegna þeirra breytinga sem verið var að vinna að þegar útfallið varð. Í umræddu kerfi […][68] og áhættumati fyrir breytinguna sést að áhrif eru metin mikil en líkur eru metnar litlar (sjá mynd 4). Þannig er ljóst að Síminn mat það sérstaklega fyrir þessa breytingarbeiðni að litlar líkur væru á að eitthvað færi úrskeiðis en ef að áhætta raungerðist yrðu afleiðingarnar miklar.

[…][69]

Mynd 4: Myndin sýnir þá breytingabeiðni í […][70] sem lá til grundvallar þeirrar uppfærslu sem var í gangi þegar útfallið varð 12. október 2021.

(54) Við skoðun Fjarskiptastofu kom í ljós að þeir kvarðar sem notaðir eru til að meta áhrif og líkur eru ólíkir eftir því hvort verið er að áhættumeta verðmæti, eða breytingarbeiðnir, sbr. kvörðun í […][71] breytingabeiðninni (mynd 4) og kvörðun í töflu úr aðferðafræði áhættumats m.a. í skjalinu „[…][72]“. Við eftirgrennslan Fjarskiptastofu á þessu misræmi svaraði Síminn því einungis til að misræmið væri til staðar, sbr. svarbréf félagsins, dags. 11. september 2023, en þar segir að *„[...]ekki [er] notast við sama kvarða í áhættumati á verðmætum annars vegar og mati á áhrifum í breytingum hins vegar, sem skýrir hið meinta ósamræmi,[...]“.*

(55) Við skoðun Fjarskiptastofu á framangreindri breytingabeiðni kom einnig í ljós að ekki virtist vera metið áhættustig eða heildarumfang áhættunnar vegna umræddra breytinga. Með bréfi, dags. 10. ágúst 2023, óskaði því Fjarskiptastofa eftir gögnum sem sýndu fram á niðurstöðu Símans á heildarumfangi áhættunnar eða áhættustigs vegna þeirra breytinga sem verið var að vinna að þegar umrætt öryggisatvik átti sér stað og hvernig komist var að þeirri niðurstöðu. Síminn svaraði því til í bréfi, dags. 11. september 2023, að:

---

[64] Heiti skjals ekki birt opinberlega.
[65] Heiti skjals ekki birt opinberlega.
[66] Hluti ákvörðunar ekki birt opinberlega.
[67] Hluti ákvörðunar ekki birt opinberlega.
[68] Hluti ákvörðunar ekki birt opinberlega.
[69] Skjáskot úr kerfum Símans ekki birt opinberlega.
[70] Hluti ákvörðunar ekki birt opinberlega.
[71] Hluti ákvörðunar ekki birt opinberlega
[72] Heiti skjals ekki birt opinberlega.

Síminn hefur þegar skilað öllum fyrirliggjandi gögnum til FST. Engin önnur gögn eru fyrir hendi í dag sem sýna fram á heildarumfang áhættunnar sem væri umfram framangreinda kvarða.

(56) Þar sem engin þeirra gagna sem Síminn hefur afhent Fjarskiptastofu sýna fram á að áhættustig hafi verið metið vegna umræddra breytinga þá verða svör Símans ekki skilinn með öðrum hætti en að slíkt mat hafi ekki farið fram.

(57) Í gagnabeiðni Fjarskiptastofu, dags. 10. ágúst 2023, fór stofnunin svo einnig fram á yfirlit yfir það hversu oft það hefur komið fyrir við mat á breytingarbeiðnum hjá Símanum að niðurstöður heildarumfangs áhættu eða áhættustigs er metið ófullnægjandi eða óviðundandi frá 12. október 2019 – 11. október 2021. Síminn svaraði því til að:

Síminn notast ekki við orðalag „ófullnægjandi" eða „óviðunandi" í tengslum við áhættumat á breytingum. Af þeim sökum er ekkert mat fyrir hendi af þeim toga sem óskað er eftir skv. orðalagi spurningar í lið c.

(58) Í þessu samhengi skal þess þó getið að við skoðun á skjölunum „[…][73]" og „[…][74]" notast Síminn við framangreint orðalag við áhættustýringu, þ.e. „ófullnægjandi" og „óviðundandi". Af því leiðir að þau skjöl eru ekki notuð í tengslum við áhættumat á breytingum. Í skjalinu „[…][75]" er svo einungis kveðið á um að breytingar skuli metnar út frá áhrifum og líkindum, ekkert er minnst á mat á áhættustigi eða heildaumfangi áhættunnar sem hlotist geta af breytingunum eða að slíkt mat eigi að fara fram.

(59) Í 7. gr. reglna nr. 1222/2007 er lögð sú skylda á fjarskiptafyrirtæki að nýta sér áhrifagreiningu og áhættumat til að draga úr öllum stærri veikleikum og veilum í innviðum sínum. Þannig skal áhrifagreining draga fram þau atvik sem geta valdið þjónusturofi. Er þar sérstaklega vísað til bilunar, óhappa eða annarra atvika sem ógna öryggi netanna og eru tiltekin í dæmaskyni mismunandi atvik sem leitt geta til þjónusturofs, svo sem bilunar í búnaði, slysa o.s.frv. Hér er ekki um tæmandi talningu að ræða og ljóst, að mati Fjarskiptastofu, að uppfærslur og aðrar breytingar í kerfum eigi hér jafnframt við.

(60) Auk framangreinds skulu fjarskiptafyrirtæki, skv. 3. mgr. ákvæðisins, framkvæma áhættumat, þ.e. meta líkindi á áhætta raungerist og hugsanleg áhrif að teknu tilliti til veikleika og fjarskiptarekstri og fjarskiptanetum. Við gerð áhættumats á grundvelli þessa ákvæðis skal fjarskiptafyrirtæki einnig fylgja ákvæði 7. gr. reglna nr. 1221/2007, við framkvæmd áhættumats á grundvelli þessa ákvæðis.

(61) Ákvæði 1. málsl. 2. tl. 7. gr. reglna nr. 1221/2007 kveður á um að fjarskiptafyrirtæki skuli skilgreina aðferðarfræði áhættumats um upplýsingaöryggi og henni fylgt eftir með skriflegu áhættumati um upplýsingaöryggi sem tengist fjarskiptanetum og fjarskiptaþjónustu. Svo segir í 2. málsl. ákvæðisins að áhættumat skuli bera kennsl á áhættuþætti, umfang þeirra og

[73] Heiti skjals ekki birt opinberlega.
[74] Heiti skjals ekki birt opinberlega.
[75] Heiti skjals ekki birt opinberlega.

forgangsraða þeim miðað við ásættanlega áhættu og þau markmið sem skipta máli fyrir fyrirtækið. Ljóst er að umrædd hugbúnaðaruppfærsla var áhættuþáttur sem tengdist fjarskiptanetum Símans sem teljast til eigna félagsins og bar félaginu því að framkvæma áhrifagreiningu og áhættumat, skv. 7. gr. reglna nr. 1222/2007 og í samræmi við 2. tl. 7. gr. reglna nr. 1221/2007.

(62) 3. málsl. 2. tl. 7. gr. reglna nr. 1221/2007, kveður á um að áhættumat skuli skilgreina eignir og gera á þeim einfalt mat og mat á þeim áhrifum sem myndast af völdum rofs á leynd, réttleika og tiltækileika. Í umræddri breytingabeiðni Símans var mat á áhrifum af völdum breytinganna á fjarskiptanet Símans í […][76] metin mikil. En eins og áður hefur komið fram teljast fjarskiptanet Símans til eigna félagsins.

(63) 4. máls. 2. tl. 7. gr. kveður svo á um að miklir veikleikar og ógnir séu skilgreindar fyrir eignirnar, ásamt mati á líkindum þeirra. Í umræddri breytingabeiðni Símans var mat á líkindum af hættu af völdum breytinganna á fjarskiptanet Símans í […][77] metin lítil.

(64) Í 5. málsl. 2. tl. 7. gr. reglna nr. 1221/2007 er kveðið á um að áhættan fyrir hvert atriði skuli reiknuð út og hún borin saman við fyrirframgerðan mælikvarða um ásættanlegt áhættustig um öryggi upplýsinga, órofinn rekstur og þjónustustig. Í umræddri breytingabeiðni var mat á áhrifum af völdum breytinganna reiknað með stigagjöfinni 3 og var matið á líkindum af hættu af völdu breytinganna reiknað með stigagjöfinni 2. Hins vegar var framangreind stigagjöf áhrifa og líkinda ekki borinn saman við fyrirframgerðan mælikvarða um ásættanlegt áhættustig og var því áhættustig umræddra breytinga ekki metið.

(65) Til þess ber einnig að líta að skv. grein 8.2 í staðlinum ISO/IEC 27001:2017[78] (hér eftir ISO 27001) segir að skipulagsheild skuli framkvæma mat á upplýsingaöryggisáhættu með fyrirfram ákveðnu millibili eða þegar verulegar breytingar eru lagðar til eða gerast. Samkvæmt grein 6.2 í framangreindum staðli þá felur slíkt mat á upplýsingaöryggisáhættu í sér m.a. ákvörðun áhættustigs. En allar breytingar sem áætlað er að taki yfir fjórðung af ári og fela í sér breytingar á grunnkerfum fjarskiptafyrirtækja teljast verulegar að mati Fjarskiptastofu og ber því á líta til umrædds ákvæðis staðalsins í þessu tilviki.

(66) Með tilliti til alls framangreinds er það niðurstaða Fjarskiptastofu að áhrif og líkur voru metin vegna umræddra breytinga en áhættustig var ekki reiknað út og borið saman við fyrirframgerðan mælikvarða um ásættanlegt áhættustig um öryggi upplýsinga, órofinn rekstur og þjónustustig og því hafi sú hætta sem steðjaði að fjarskiptaneti Símans ekki verið áhættumetin með fullnægjandi hætti þegar umrætt öryggisatvik átti sér stað. En slíkt er ekki í samræmi við þær skyldur sem hvíla á fjarskiptafyrirtækjum skv. 1. mgr. 7. gr. reglna nr. 1222/2007, sbr. 5. málsl. 2. tl. 7. gr. reglna nr. 1221/2007.

4.4.2 Breytingastjórnun

Almennt

[76] Hluti ákvörðunar ekki birt opinberlega.
[77] Hluti ákvörðunar ekki birt opinberlega.
[78] Sú útgáfu staðalsins sem var í gildi þegar atvik máls áttu sér stað.

(67) Í gagnabeiðni Fjarskiptastofu þann 6. maí 2022 var beðið um afrit af skjalfestum verkferlum við breytingastjórnun. Í kjölfar beiðninnar afhenti Síminn þann 24. maí 2022 skjalið „[…][79]“, en skjalið lýsir ferli breytingastjórnunar og er þar farið yfir samþykktarferlið, fjallað um breytingaráð og fleiri þætti sem varða breytingastjórnun hjá fyrirtækinu. Síminn afhenti svo Fjarskiptastofu í kjölfar síðari gagnabeiðni stofnunarinnar, dags. 11. september 2023, skjölin „[…][80]“, „Fundargerð_34_2021.docx“, „Fundargerð_35_2021.docx“ og 21 fundargerð [birgis og þjónustuveitanda Símans][81] vegna funda sem haldnir voru milli Símans og [birgis og þjónustuveitanda Símans][82].

Breytingin

(68) Í svarbréfi Símans, dags 23. maí 2022, segir að fjallað hafi verið um breytinguna og hún samþykkt á fundi breytingaráðs Símans þann 26. ágúst 2021. Í fundargerð breytingaráðs nr. 34/2022 þar sem umrædd breytinga var samþykkt segir eftirfarandi um hana:

> *[…][83]. Stór uppfærsla í […][84]. Uppfærslan tekur langan tíma, um 7 vikur skv. nýjustu upplýsingum. Að þeim tíma loknum verður samsvarandi búnaður í [….][85] uppfærður.*

(69) Í frávikaskýrslu Símans, sbr. skjalið „[…][86]“, segir svo eftirfarandi um breytinguna:

> *Farsímakjarni Símans […][87]. Stór hluti kerfins keyrir í […][88] sem framleiðandi kerfisins er að uppfæra í […][89] [90] og á meðan er umferð að keyra í […][91].*

(70) Svo segir í frávikaskýrslu [birgis og þjónustuveitanda Símans][92], dags. 17. desember 2021, um breytinguna:

> *As a part of the Siminn […][93] upgrade project[94], due to troouplesh ooting 11:30 GMT, [birgir og þjónustuveitandi Símans][95] by human mistake changed/modified the […][96][...]*

[79] Heiti skjals ekki birt opinberlega.
[80] Heiti skjalanna ekki birt opinberlega.
[81] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[82] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[83] Hluti bréfs ekki birt opinberlega.
[84] Hluti bréfs ekki birt opinberlega, þ.m.t. nafn birgis og þjónustuveitanda Símans.
[85] Hluti bréfs ekki birt opinberlega.
[86] Nafn skjals ekki birt opinberlega.
[87] Hluti frávikaskýrslu ekki birt opinberlega.
[88] Hluti frávikaskýrslu ekki birt opinberlega.
[89] Hluti frávikaskýrslu ekki birt opinberlega.
[90] Undirstrikun Fjarskiptastofu.
[91] Hluti frávikaskýrslu ekki birt opinberlega.
[92] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[93] Hluti frávikaskýrslu ekki birt opinberlega.
[94] Undirstrikun Fjarskiptastofu.
[95] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[96] Hluti frávikaskýrslu ekki birt opinberlega.

(71) Samkvæmt gögnum málsins fólst því í umræddri breytingu að [birgir og þjónustuveitandi Símans][97] var í samstarfi við Símann að uppfæra […][98], en um var að ræða […][99] uppfærsla úr […][100]. Skv. verkáætlun (sjá mynd 6 á bls. 24) átti heildaruppfærslan í farsímakjarna Símans […][101] að taka yfir 14 vikur eða um fjórðung árs 2021 og var því um verulega uppfærslu að ræða. Af gögnum málsins leiðir einnig að verið var að vinna í umræddri breytingu þegar öryggisatvikið átti sér stað og að umrædd breyting á kerfum Símans var framkvæmd af [birgi og þjónustuveitanda Símans][102] í samstarfi við Símann.

Útvistun

(72) Af gögnum málsins leiðir að ríkt samstarf er milli Símans og [birgi og þjónustuveitanda Símans][103] og er sá síðarnefndi framleiðandi þess kerfis sem verið var að uppfæra og var félagið að framkvæma breytingar á kerfum Símans þegar umrætt öryggisatvik átti sér stað. En fram kemur í fundargerðum [birgis og þjónustuveitanda Símans][104] vegna funda þess við Símann að mikið samstarf var milli félaganna m.a. hafði [birgir og þjónustuveitandi Símans][105] framkvæmt ýmsar uppfærslu fyrir kerfi Símans rétt áður en umrætt öryggisatvik átti sér stað.[106]

(73) Síminn afhenti Fjarskiptastofu þann 11. september 2023 þjónustusamning ([…][107]) sem var í gildi milli Símans og [birgis og þjónustuveitanda Símans][108] þegar umrætt öryggisatvik átti sér stað, sbr. skjalið „[…][109]“, og er samningurinn dagsettur í desember 2014. Í viðaukum við samninginn er kveðið á um margskonar aðstoð, ráðgjöf og vinnu sem [birgir og þjónustuveitandi Símans][110] getur framkvæmt fyrir Símann varðandi fjarskiptanet félagsins. Í kafla 3.1.1 viðauka við þjónustusamninginn ([…][111]), sbr. skjalið „[…][112]“, er kveðið á um það að [birgir og þjónustuveitandi Símans][113] veiti Símanum aðstoð og ráðgjöf varðandi fjarskiptanet félagsins ([…][114]). Einnig er kveðið á um svokallað „[…][115]“ í kafla 3.1.2 framangreinds viðauka sem getur falið í sér að [birgir og þjónustuveitandi Símans][116] veitir ráðgjöf og aðstoð varðandi slíka aðgerðir og að félagið geti einnig framkvæmt slíkar aðgerðir fyrir Símann ef farið er fram á það. Svo er í framangreindum viðauka kveðið á um svokallað

97 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
98 Hluti ákvörðunar ekki birt opinberlega.
99 Hluti frávikaskýrslu ekki birt opinberlega.
100 Hluti ákvörðunar ekki birt opinberlega.
101 Hluti ákvörðunar ekki birt opinberlega.
102 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
103 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
104 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
105 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
106 Sjá m.a. bls. 4 í skjalinu "Minutes of meeting 2021-03-17. pdf" og bls. 4 í skjalinu „Minutes of meeting 2021-04-07.pdf".
107 Heiti þjónustusamningsins ekki birt opinberlega.
108 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
109 Heiti skjals ekki birt opinberlega.
110 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
111 Heiti viðauka þjónustusamningsins ekki birt opinberlega.
112 Heiti skjals ekki birt opinberlega.
113 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
114 Hluti ákvörðunar ekki birt opinberlega.
115 Hluti ákvörðunar ekki birt opinberlega.
116 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

„[…][117]“ í kafla 3.1.3 og „[…][118]“ í kafla 3.1.4. […][119]. Í sérstökum viðauka eða breytingum við þjónustusamninginn ([…][120]), sbr. skjalið „[…][121]“, er svo kveðið á um frekari þjónustu sem [birgir og þjónustuveitandi Símans][122] veitir Símanum m.a. varðandi framkvæmd uppsetningar og uppfærslna fyrir kerfi Símans sem varða fjarskiptanet félagsins[123].

(74) Þess skal getið að með bréfi Fjarskiptastofu, dags. 10. ágúst 2023, óskað stofnunin eftir afriti af verkferlum félagsins, sem í gildi var þann 12. október 2021, fyrir gangsetningu áfallalausna. Í bréfi Símans, dags. 11. september 2023, er framangreindri spurningu svarað með eftirfarandi hætti:

[…][124]

(75) Af þessum ummælum verður ekki annað ráðið en að [birgir og þjónustuveitandi Símans][125] sjái […][126] sem hluta umrædds þjónustusamnings.

(76) Sú þjónusta sem rakin hefur verið hér að framan, og er andlag framangreinds þjónustusamnings og viðauka hans, varðar bæði kerfisbundna aðstoð og ráðgjöf auk framkvæmd vinnu við uppfærslur og uppsetningar í tengslum við fjarskiptanet Símans, en allt eru þetta þættir sem nauðsynlegir eru fyrir rekstur fjarskiptanets. En Síminn segir í bréfi, dags. 11. september 2023, að hann kaupi *„[...] þjónustu frá [birgi og þjónustuveitandi Símans][127] sem tengist rekstri Símans á farsímakerfum sínum, á grundvelli þjónustusamnings, og hefur gert til fjölda ára.“*. Sú vinna sem [birgir og þjónustuveitandi Símans][128] framkvæmdi fyrir Símann á grundvelli umrædds þjónustusamnings varðaði því rekstur fjarskiptaneta félagsins.

(77) Það er einnig mat Fjarskiptastofu að þar sem [birgir og þjónustuveitandi Símans][129] veitir Símanum kerfisbundna aðstoð og ráðgjöf auk þess að framkvæma vinnu við uppfærslur og uppsetningar í tengslum við fjarskiptanet félagsins þá sinni [birgir og þjónustuveitandi Símans][130], á grundvelli framangreinds þjónustusamnings, starfsemi sem er nauðsynleg fyrir a.m.k. virkni fjarskiptaneta Símans. En í andmælabréfi Símans, dags. 15. febrúar 2023, kemur m.a. fram að „[í] *samningi Símans við [birgi og þjónustuveitanda Símans][131] er meðal annars*

[117] Hluti ákvörðunar ekki birt opinberlega.
[118] Hluti ákvörðunar ekki birt opinberlega.
[119] Hluti ákvörðunar ekki birt opinberlega.
[120] Heiti viðauka við þjónustusamning ekki birt opinberlega.
[121] Heiti skjalsins ekki birt opinberlega.
[122] Nafn birgis og þjónustuveitanda Símans er ekki birt opinberlega.
[123] Sjá t.d. […] og bls. 124 (kafli 1.2.5 í Annex 7) í skjalinu „[…]“
[124] Hluti bréfs ekki birt opinberlega.
[125] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[126] Hluti ákvörðunar ekki birt opinberlega.
[127] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[128] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[129] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[130] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[131] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

fjallað um þá þjónustu sem [birgir og þjónustuveitandi Símans][132] veitir Símanum í tengslum við viðhald og uppfærslur á búnaði til að tryggja virkni þess,[...]*".*

(78) Þar sem Síminn hefur gert þjónustusamning við [birgi og þjónustuveitanda Símans][133] sem varðar rekstur fjarskiptaneta félagsins sem felur í sér starfsemi sem a.m.k. er nauðsynleg fyrir virkni fjarskiptaneta félagsins þá verður ekki komist að annarri niðurstöðu, með hliðsjón af framangreindu, en að Síminn hafi samið við [birgi og þjónustuveitanda Símans][134] um að annast rekstur fjarskiptaneta sinna að hluta með gerð framangreinds þjónustusamnings og þar með sé um að ræða útvistun á rekstri fjarskiptaneta Símans í skilningi 13. gr. reglna nr. 1221/2007. En það að fjarskiptafyrirtæki gerir samning við þriðja aðila um að sinna starfsemi sem nauðsynleg er fyrir virkni fjarskiptanets þess, felur í sér að útvistun reksturs, þar sem sú starfsemi sem um ræðir er ekki framkvæmd af fyrirtækinu sjálfu en er samt nauðsynleg fyrir virkni fjarskiptanes þess.

(79) Við yfirferð Fjarskiptastofu á umræddum þjónustusamningi ásamt viðaukum hans, kom í ljós að ekki var kveðið á um skyldu [birgis og þjónustuveitanda Símans][135] til að starfa í samræmi við fyrirmæli Símans og ákvæði reglna nr. 1221/2007. Einnig var þar ekki að finna ákvæði sem tryggðu Fjarskiptastofu aðgang að upplýsingum frá [birgi og þjónustuveitanda Símans][136] og að stofnunin geti í þágu eftirlits framkvæmt athuganir á starfsstöð þess, og að lokum var þar ekki að finna ákvæði um þagnarskyldu og þar með tryggt að farið sé að ákvæðum fjarskiptalaga þar að lútandi. Að vísu voru þar ákvæði um þagnarskyldu er vörðuðu samninginn sjálfan en ekki var þar kveðið á um þagnarskyldu í samræmi við 47. gr. þágildandi fjarskiptalaga. Af því leiðir að umræddur þjónustusamningur Símans við [birgi og þjónustuveitanda Símans][137] var ekki í samræmi við þær kröfur sem leiða af 1., 3. og 5. tl. 13. gr. reglna nr. 1221/2007.

<u>Samþykktarferli breytinga</u>

(80) Fjarskiptastofa óskaði upplýsinga um hvernig staðið hefði verið að samþykki Símans á breytingunum sem orsökuðu útfalli 12. október 2021 í bréfi, dags. 6. maí 2022. Í svörum Símans sagði að fjallað hefði verið um breytinguna og hún samþykkt á fundi breytingaráðs Símans þann 26. ágúst 2021, þ.e. tæpum tveimur mánuðum áður en að breyting var framkvæmd og við upphaf nokkuð langs breytingatímabils.

(81) Í svarbréfi Símans, dags. 23. maí 2022, kemur fram skjáskot af breytingabeiðni (sjá mynd 4) vegna þess verks sem verið var að vinna þegar umrætt öryggisatvik átti sér stað. Með bréfi, dags. 10. ágúst 2023, er vísað til þessa skjáskots og óskaði Fjarskiptastofa eftir frekari gögnum um beiðnina, þ.e. afriti af samþykktri breytingabeiðni vegna þess verks sem verið var að vinna þegar umrætt öryggisatvik átti sér stað 12. október 2021 þar sem allar upplýsingar er varða

[132] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[133] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[134] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[135] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[136] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[137] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

hana koma fram. Í svarbréfi Símans, dags. 11. september 2023, var spurningunni svarað með eftirfarandi hætti:

> *Mistökin eru gerð samhliða stóru uppfærsluverkefni sem er samþykkt í heild sinni, en ekki hvert smáatriði í kerfi sem er ekki tengt umheiminum á meðan á því stendur. Þessar upplýsingar býr FST nú þegar yfir[138]. Í verkefni sem þessu þá vinna sérfræðingar Símans á móti sérfræðiteymi [birgis og þjónustuveitanda Símans][139] og ákveður teymið hvað skal gert á hverjum tíma. Það var yfirleitt gert með […][140] og stærri ákvarðanir svo settar í fundargerðir, sem fylgja hér með svarbréfi þessu (vísað til sem „[birgis og þjónustuveitanda Símans][141] fundargerðirnar") frá árinu 2021.*

(82) Ályktaði Fjarskiptastofa út frá þessum svörum Símans við skýrri spurningu stofnunarinnar að engin frekari gögn væru því til varðandi breytingarbeiðnina önnur en þau sem Fjarskiptastofa hafði þegar í sinni vörslu. Hins vegar kom í ljós í andmælabréfi Símans, dags. 18. janúar 2024, að fyrir mistök hafði félagið ekki sent Fjarskiptastofu allt skjáskotið af breytingarbeiðni þeirri er lá til grundvallar þeim breytingum sem verið var að vinna að þegar öryggisatvikið átti sér stað. En í því skjáskoti sem stofnuninn hafði undir höndum (mynd 4) vantaði bæði stutta lýsingu á breytingunni og dagsetningar og var skjáskot sent með bréfi Símans sem innihélt þau atriði.

(83) Verklagsreglur Símans um breytingarstjórnun sem í gildi voru þegar atvik máls áttu sér stað, sbr. skjalið „[…][142]"[143] kváðu á um að breytingar á búnaði og kerfum Símans skuli stýrt með formlegum og skjöluðum hætti. Um form og efni breytingabeiðna giltu svo verklagsreglur Símans „[…][144]"[145]. Í framangreindum verklagsreglum kemur fram listi yfir þau helstu atriði sem fram eiga að koma í breytingabeiðni. Þar er m.a. kveðið á um að koma skuli fram stutt lýsing á umræddri breytingu […][146]. Í listanum kemur einnig fram að í breytingarbeiðni skuli því vera […][147]. Ekki er kveðið á um framangreind atriði í þeirri breytingarbeiðni er Fjarskiptastofa hefur undir höndum, að vísu er þar stutt lýsingu á umræddri breytingu en þar var ekki reynt að meta alvarleika út frá fjöldi viðskiptavina með þjónustu, miðlæg/staðbundin áhrif og lykilviðskiptavini sem verða fyrir áhrifum. Er það því mat Fjarskiptastofu að breytingarbeiðnin sé takmörkuð og óljós. Hins vegar er ekki hægt að fullyrða að Síminn hafi þar með brotið gegn sínum eigin verklagsreglum þar sem þær kveða ekki með skýrum hætti á um hvaða atriði lista framangreindra verklagsreglna Símans „[…][148]"[149], breytingarbeiðnir skuli innhalda eða hvernig meta skuli hvaða atriði hans skuli skrá í breytingarbeiðnir félagsins.

[138] Undirstrikun Fjarskiptastofu.
[139] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[140] Hluti bréfs ekki birt opinberlega.
[141] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[142] Heiti skjals ekki birt opinberlega.
[143] Útg. 4.0, bls. 1.
[144] Heiti verklagsreglnanna ekki birt opinberlega.
[145] Útg. 3.0
[146] Hluti ákvörðunar ekki birt opinberlega.
[147] Hluti ákvörðunar ekki birt opinberlega.
[148] Heiti verklagsreglnanna ekki birt opinberlega.
[149] Útg. 3.0

Einungis segir í verklagsreglum Símans að *„[þ]egar starfsmaður er ánægður með skráninguna […][150]““.*

(84) Það að framangreindar verklagsreglur Símans séu orðaðar með jafn óskýrum hætti og raun ber vitni um jafn mikilvægt atriði og um hvaða atriði breytingarbeiðnir skuli innihalda, felur í sér að nær ómögulegt er að átta sig á hlítni við þær. Af þeim sökum ná þær ekki markmiði verkferla um breytingar að tryggja traustan, skipulegan og fyrirsjáanlegan rekstur fjarskiptaneta í samræmi við 2. málsl. 1. mgr. 23. gr. reglna nr. 1222/2007.

(85) Það að Síminn skuli ekki kveða með skýrum hætti á um það í verklagsreglum sínum hvaða efnisatriði breytingabeiðnir félagsins skuli innihalda eða hvernig meta eigi hvaða efnisatriði hún skuli innihalda, getur því ekki falið í sér traustan, skipulegan og fyrirsjáanlegan rekstur fjarskiptaneta. Þar með er það mat Fjarskiptastofu að framangreindar verklagsreglur Símans séu ekki í samræmi við þær kröfur sem leiða af 1. mgr. 23. gr. reglna nr. 1222/2007.

<u>Framkvæmd breytinganna</u>
Almennt
(86) Fjarskiptastofa spurði Símann í bréfi stofnunarinnar, dags. 6. maí 2022, um það með hvaða hætti kröfur um upplýsingaöryggi, m.a. breytingarstjórnun væri miðlað til [birgis og þjónustuveitanda Símans][151] (þriðja aðila). Í svörum Símans sagði að reglulegir fundir væru með framleiðanda ([birgis og þjónustuveitanda Símans][152]) hvað varðar "Support and maintenance", á þeim fundum eru m.a. skipulagðar uppfærslur á kerfum. Því til staðfestingar fylgdu fundargerðir [birgis og þjónustuveitanda Símans][153] vegna funda sem haldnir voru milli Símans og [birgis og þjónustuveitanda Símans][154] árið 2021 og vegna eins fundar 2022. Í öllum fundargerðunum er talað um tilgang fundanna, en um er að ræða stöðufundi vegna uppfærslna til að ákvarða næstu skref, sbr. texta á mynd 5.

[…][155]

Mynd 5: Myndin sýnir texta úr fundargerðinni „Minutes of meeting 2021-10-13.pdf“ þar sem tilgangur fundarins er tíundaður.

(87) Í fundargerðarskjalinu: „Minutes of meeting 2021-10-13.pdf" kemur fram verkáætlun um uppfærslu kerfa í […][156]. Síminn sendi svo Fjarskiptastofu sömu verkáætlun sem svar við gagnabeiðni stofnunarinnar þann 11. september 2023 þar sem búið er að rauðlita það verk sem verið var að vinna að þegar umrætt öryggisatvik átti sér stað (mynd 6). Þar sést að í meira en 14 vikur er áætlað að vinna að breytingum í lykilkerfum félagsins.

[150] Hluti verklagseglnanna ekki birt opinberlega.
[151] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[152] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[153] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[154] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[155] Hluti fundargerðar ekki birt opinberlega.
[156] Hluti ákvörðunar ekki birt opinberlega.

[…][157]

Mynd 6: Myndin sýnir verkáætlun fyrir uppfærslu kerfa í […][158] og […][159] eins og hún birtist í svarbréfi Símans, dags. 11. september 2023.

(88) Hér er um töluvert langan tíma að ræða eða yfir fjórðung ársins 2021 þar sem annað af mikilvægustu kerfum félagsins er […][160].

(89) Eins og fram hefur komið þá fólust breytingarnar í því að [birgir og þjónustuveitandi Símans][161] var í samstarfi við Símann að uppfæra […][162] félagsins í […][163], en um var að ræða […][164] uppfærsla úr […][165]. Í fundargerð [birgis og þjónustuveitanda Símans][166] vegna fundar félagsins við Símann, sbr. skjalið „Minutes of meeting 2021-10-13.pdf", degi eftir umrætt öryggisatvik, segir eftirfarandi:

> *Yesterday [birgir og þjónustuveitandi Símans][167] started initial testing to troubleshoot […][168].*
>
> *For troubleshooting a […][169] and […][170] was modified[171]. Unfortunately changes were committed/saved and thus the same got replicated […][172], which impacted […][173]. This resulted in […][174].*

(90) Af framangreindu leiðir að þegar meint öryggisatvik átti sér stað var [birgir og þjónustuveitandi Símans][175] að vinna í því að vandræðaveiða (troubleshooting) í farsímakjarnanum í […][176] til að kanna hvort uppfærslan þar hefði heppnast. En við þá vinnu voru ákveðnar breytingar vistaðar sem höfðu áhrif á farsímakjarnann í […][177], sem var að þjónusta viðskiptavini, sem orsakaði útfallið.

---

157 Hluti fundargerðar ekki birt opinberlega.
158 Hluti ákvörðunar ekki birt opinberlega.
159 Hluti ákvörðunar ekki birt opinberlega.
160 Hluti ákvörðunar ekki birt opinberlega.
161 Nafn birgis og þjónustuveitanda Símans er ekki birt opinberlega.
162 Hluti ákvörðunar ekki birt opinberlega.
163 Hluti ákvörðunar ekki birt opinberlega.
164 Hluti ákvörðunar ekki birt opinberlega.
165 Hluti ákvörðunar ekki birt opinberlega.
166 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
167 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
168 Hluti fundargerðar ekki birt opinberlega.
169 Hluti fundargerðar ekki birt opinberlega.
170 Hluti fundargerðar ekki birt opinberlega.
171 Undirstrikun Fjarskiptastofu.
172 Hluti fundargerðar ekki birt opinberlega.
173 Hluti fundargerðar ekki birt opinberlega.
174 Hluti fundargerðar ekki birt opinberlega.
175 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
176 Hluti ákvörðunar ekki birt opinberlega.
177 Hluti ákvörðunar ekki birt opinberlega.

(91) Í bréfi Fjarskiptastofu, dags. 10. ágúst 2023, óskaði Fjarskiptastofa eftir skýringum á því hvers vegna ekki hafi verið tryggt að engin tenging væri milli farsímakjarna Símans í […][178] á meðan unnið var að breytingum í […][179]. Í svarbréfi Símans, dags. 11. september 2023, kemur m.a. eftirfarandi fram:

> *Þegar atvikið á sér stað er uppfærslum lokið á öllum kerfunum í […][180] [181] og á þeim tímapunkti er búið að samtengja kerfin[182], þó svo að kerfin í […][183] hafi ekki verið byrjuð að taka umferð.*

(92) Í bréfi Fjarskiptastofu, dags. 10. ágúst 2023, þá óskaði stofnunin svo skýringa á því hvaða hluti farsímakjarna Símans í […][184] hafi verið virkur og hvers vegna. Í svarbréfi Símans, dags. 11. september 2023, er spurningu Fjarskiptastofu svarað með eftirfarandi hætti:

> *Enginn hluti farsímakjarna Símans í […][185] var virkur, þ.e.a.s. með þeim hætti að hann væri að þjónusta viðskiptavini. Hins vegar er hann „virkur" í þeim skilningi að kveikt var á honum, enda verið að vinna í breytingunni á þessum tíma. Eins og segir hér ofar í skýringum félagsins við spurningu 5, þá var verið að undirbúa það að taka […][186] í notkun, enda uppfærslum lokið, […][187] [188] þó svo að […][189] væri ekki að afgreiða umferð, þ.e. „óvirkur".*

(93) Fjarskiptastofa óskaði einnig eftir afriti þeirra prófana sem fram fóru áður en framkvæmdar voru þær breytingar í kerfum Símans sem ollu umræddu öryggisatviki í gagnabeiðni, dags. 10. ágúst 2023. Síminn svaraði því til í svarbréfi, dags. 11. september 2023, að slíkar prófanir hefðu ekki farið fram og svo segir þar jafnframt eftirfarandi:

> *Á þeim tímapunkti sem atvikið á sér stað er verkefnið á lokastigum, þ.e. verið var að undirbúa samkeyrslu kerfanna á nýjan leik að lokinni uppfærslu.*

(94) Af framangreindu leiðir að tenging var komin milli farsímakjarna Símans í […][190] þegar [birgir og þjónustuveitandi Símans][191] var að vinna í vandræðaveiðum eftir að umræddri uppfærslu var lokið í […][192], og verið var að undirbúa samkeyrslu […][193]. Hér er því um að ræða mjög áhættusaman hluta uppfærslunnar þar sem tenging er kominn milli farsímakjarnanna,

---

[178] Hluti ákvörðunar ekki birt opinberlega.
[179] Hluti ákvörðunar ekki birt opinberlega.
[180] Hluti bréfs ekki birt opinberlega.
[181] Með tölvubréfi, dags. 8. nóvember 2023, staðfesti Síminn að hér væri átt við […].
[182] Undirstrikun Fjarskiptastofu.
[183] Hluti bréfs ekki birt opinberlega.
[184] Hluti ákvörðunar ekki birt opinberlega.
[185] Hluti bréfs ekki birt opinberlega.
[186] Hluti bréfs ekki birt opinberlega.
[187] Hluti bréfs ekki birt opinberlega.
[188] Undirstrikun Fjarskiptastofu.
[189] Hluti bréfs ekki birt opinberlega.
[190] Hluti ákvörðunar ekki birt opinberlega.
[191] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[192] Hluti ákvörðunar ekki birt opinberlega.
[193] Hluti ákvörðunar ekki birt opinberlega.

en umrætt öryggisatvik gerðist einmitt við þennan verkþátt. Af gögnum málsins má þó sjá að eftir að öryggisatvik kom upp fór [birgir og þjónustuveitandi Símans][194] beint í að bakka með breytinguna. Er því ljóst að endurheimtarferlar voru til staðar. Í fundargerð [birgis og þjónustuveitanda Símans][195] kemur fram að eftir bilunina var tekin ákvörðun um að fresta frekari uppfærslum fram í […][196] (mynd 7 og 8).

[…][197]

Mynd 7: Myndin sýnir texta úr skjalinu: „ Minutes of meeting 2021-10-13“ þar sem fram kemur fram næstur skref í uppfærslunni.

[…][198]

Mynd 8: Myndin sýnir texta úr skjalinu: „ Minutes of meeting 2021-10-13“ þar sem fram kemur að frekari uppfærslum er frestað þar til í […][199].

Venja Símans

(95) Ljóst er að umfangsmikið útfall varð á þjónustu Símans við umrætt öryggisatvik. Í frávikaskýrslu þeirri sem Fjarskiptastofu barst frá Símanum þann 19. október 2021 kemur fram að til að fyrirbyggja að atvik sem þetta geti komið upp að nýju verði farið yfir ferla með framleiðanda búnaðarins sem og að framkvæma skuli allar breytingar sem gætu haft áhrif á neytendur að nóttu til eins og venjan er hjá Símanum. En í skýrslunni segir að: *„*[a]*llar configbreytingar skoðaðar í þaula og allar breytingar sem hugsanlega hafa áhrif á notendur skulu gerðar að nóttu til eins og venjan er hjá Símanum.“.*

(96) Fjarskiptastofa spurði nánar um framangreinda venju Símans í bréfi, dags. 10. ágúst 2023 og í svarbréfi Símans, dags. 11. september 2023, kemur fram að framangreind venja Símans sé ekki hluti af verkferlum Símans sem hafi hlotið viðeigandi samþykki. Af því leiðir að framangreind venja, sem felur í sér verkferla um hvenær breytingar eru heimilaðar í kerfum Símans svo að þær trufli sem minnst þjónustu félagsins, hefur ekki verið skjalfest og er ekki skráð í verklagsreglur breytingarstjórnunar hjá Símanum. Það er mat Fjarskiptastofu að sú efnisregla sem fellst í umræddri venju feli í sér mikilvæga meginreglu um það hvenær framkvæma eigi breytingar hjá Símanum. Það að slík meginregla skuli ekki vera hluta af formlegum skjalfestum verklagsreglum Símans um framkvæmd breytinga felur í sér að félagið hafi ekki tryggt að verkferlar sem fjalla um breytingar feli í sér viðeigandi formlega

[194] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[195] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[196] Hluti ákvörðunar ekki birt opinberlega.
[197] Hluti fundargerðar ekki birt opinberlega.
[198] Hluti fundargerðar ekki birt opinberlega.
[199] Hluti ákvörðunar ekki birt opinberlega.

meðhöndlun breytinga ásamt skjalfestingu þeirra og er slíkt ekki í samræmi við kröfur 1. mgr. 23. gr. reglna nr. 1222/2007.

(97) Í andmælabréfi Símans, dags. 15. febrúar 2023, kemur fram að umrædd venja eigi ekki við þegar unnið er í kerfum sem eru ekki virk. En þar segir m.a.:

> *Það var verið að vinna í kerfi sem var í viðhaldi og hafði á þeim tíma engin áhrif fyrir neytendur. […][200] var til staðar og þar af leiðandi átti umrædd framkvæmd ekki að hafa áhrif á neytendur. Hvenær unnið var í hinu […][201] hefur einfaldlega enga þýðingu í málinu.*

(98) Það er hins vegar ljóst af gögnum málsins að tenging var kominn milli farsímakjarna Símans í […][202] þegar umrædd vinna við uppfærsluna átti sér stað þann 12. október 2021, þar sem verið var að undirbúa það að færa umferð […][203]. Ekki er því hægt að segja að farsímakjarni Símans í […][204] hafi verið óvirkur með öllu þegar öryggisatvikið átti sér stað, því þó stöðin hafi ekki verið að þjónusta viðskiptavini í farsímakerfi Símans á umræddum tíma, var hún enga síður með tengingu við farsímakjarna Símans í […][205].

(99) Í andmælabréfi Símans, dags. 15. febrúar 2023, kemur einnig fram að:

> *Sú venja Símans sem FST vísar til varðar þau tilvik sem Síminn þarf að slökkva á lifandi kerfum þannig að kerfin verða óaðgengileg fyrir notendur. Það var ekki tilfellið í þessu máli.*

(100) Einnig kemur eftirfarandi fram í andmælabréfi Símans, dags. 18. janúar 2024:

> *„[...]hefur venja félagsins náð til tilvika þegar stendur til að „slökkva“ á virkum, lifandi kerfum sem gætu þar með haft áhrif á þjónustu til viðskiptavina Símans.“*

(101) Af framangreindu leiðir að þrátt fyrir að venja Símans sé orðuð afdráttarlaust í frávikaskýrslu félagsins, þá verður ekki hægt að fullyrða að Símann hafi brotið gegn venju sinni í umrætt sinn vegna þeirra nýju upplýsinga sem bárust í framangreindum andmælabréfum. En Síminn segir þar að venjan gildi einungis um þau tilvik þegar stendur til að „slökkva“ á virku, lifandi kerfum sem gæti haft áhrif á þjónustu til viðskiptvina félagsins. Hins vegar kváðu verklagsreglur Símans ekki á um þá venju félagsins að framkvæma skyldi allar breytingar sem gætu haft áhrif á notendur að nóttu til a.m.k. þegar stendur til að „slökkva“ á virku, lifandi kerfum sem gæti haft áhrif á þjónustu til viðskiptavina félagsins. Af framangreindu leiðir því að verkferlar Símans sem fjölluðu um breytingar tryggðu ekki viðeigandi formlega meðhöndlun breytinga ásamt skjalfestingu þeirra en slíkt er ekki í samræmi við kröfur 1. mgr. 23. gr. reglna nr. 1222/2007.

[200] Hluti bréfs ekki birt opinberlega.
[201] Hluti bréfs ekki birt opinberlega.
[202] Hluti ákvörðunar ekki birt opinberlega.
[203] Hluti ákvörðunar ekki birt opinberlega.
[204] Hluti ákvörðunar ekki birt opinberlega.
[205] Hluti ákvörðunar ekki birt opinberlega.

Aðgangsstýring

(102) Eins og fram hefur komið þá fólust umræddar breytingar í því að starfsmaður [birgis og þjónustuveitanda Símans][206] var að vinna í uppfærslu á […][207] Símans […][208]. Ljóst er að hann var að vinna í uppfærslunni um miðjan dag. Óskaði Fjarskiptastofa því upplýsinga í bréfi, dags. 6. maí 2022, hvernig aðgangsheimildum [birgis og þjónustuveitanda Símans][209] væri háttað inn í kerfi félagsins. Í svörum Símans, dags. 23. maí 2022, sagði eftirfarandi:

> *[…][210]. Aðgangur og vinnubrögð o.s.frv. er í samræmi við þjónustusamninga á hverjum tíma[211].*

(103) Fjarskiptastofa óskaði einnig eftir upplýsingum um hvernig tímamörk og breytingaheimildir á aðgangi [birgis og þjónustuveitanda Símans][212] hafi verið háttað á þeim tíma sem atvikið varð. Í svörum Símans, dags. 23. maí 2022, segir að *„[…][213]“*.

(104) Til áréttingar svari Símans þann 23. maí 2022 fylgdu svo í viðhengi eftirfarandi fjögur skjöl: „[…][214]“. Í framangreindum viðaukum er m.a. fjallað um að [birgir og þjónustuveitandi Símans][215] og viðskiptavinurinn […][216]. Einnig er fjallað um kröfur [birgis og þjónustuveitanda Símans][217] um nokkuð […][218] svo fyrirtækið geti sinnt starfi sínu fyrir viðskiptavini sína, en þar segir m.a.:

[…][219]

(105) Ekki er að finna í umræddum gögnum að Síminn setji fram með skriflegum hætti ramma um það hvenær sólarhringsins [birgir og þjónustuveitandi Símans][220] framkvæmir breytingar í kerfum félagsins svo það trufli sem minnst þjónustu til viðskiptavina þeirra. Virðist sá tímarammi sem um ræðir í raun ná til alls breytingartímabilsins. Þess skal þó getið að allir framangreindir viðaukar við þjónustusamninginn eru dagsettir eftir að atvik máls áttu sér stað eða 1. janúar 2022, fyrir utan skjalið „[…][221]“. Hins vegar kemur fram í andmælabréfi Símans, dags. 18. janúar 2024, að þegar öryggisatvikið átti sér stað hafi verið til staðar efnislega sambærilegir viðaukar við þjónustusamning Símans við [birgi og þjónustuveitanda Símans][222] og þeir viðaukar sem Síminn hafði afhent stofnuninni. En í þeim þjónustusamningi sem

[206] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[207] Hluti ákvörðunar ekki birtur opinberlega.
[208] Hluti ákvörðunar ekki birtur opinberlega.
[209] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[210] Hluti bréfs ekki birtur opinberlega.
[211] Undirstrikun Fjarskiptastofu.
[212] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[213] Tilvitnun ekki birt opinberlega.
[214] Heiti skjala ekki birt opinberlega.
[215] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[216] Hluti ákvörðunar ekki birtur opinberlega.
[217] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[218] Hluti ákvörðunar ekki birtur opinberlega.
[219] Tilvitnun ekki birt opinberlega.
[220] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[221] Heiti skjals ekki birt opinberlega.
[222] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

afhentur var Fjarskiptastofu og var í gildi þegar atvik máls eiga sér stað er þó einungis kveðið á um að Síminn skuli […][223] aðgang að kerfum sínum til að þeir geti framkvæmt þá þjónustu sem þar er samið um.

(106) Í andmælabréfi Símans, dags. 15. febrúar 2023, kemur fram að […][224] í þau kerfi sem þjónusta skv. þjónustusamningi tók til og nái til a.m.k. […][225] og að [birgir og þjónustuveitandi Símans][226] hafði […][227], en þar segir:

> *Í samningi Símans við [birgi og þjónustuveitanda Símans][228] er meðal annars fjallað um þá þjónustu sem [birgir og þjónustuveitandi Símans][229] veitir Símanum í tengslum við viðhald og uppfærslur á búnaði til að tryggja virkni þess, og þar með samtengdra kerfa og atvikaskráningum, sem og viðbrögðum af hálfu [birgis og þjónustuveitanda Símans][230] í þeim tilvikum sem við á. <u>Til að geta veitt slíka þjónustu á grundvelli samningsins er nauðsynlegt að [birgir og þjónustuveitandi Símans][231] hafi […][232] aðgang að þeim kerfum sem þjónusta þess tekur til. Sökum þessa er sérstaklega kveðið á um það í samningnum að […][233].</u>[234]*

(107) Í bréfi segir einnig að:

> *[Birgir og þjónustuveitandi Símans[235]] starfar því eftir þeim fyrirmælum Símans að tryggja viðeigandi og nauðsynlega þjónustu samkvæmt samningi, <u>en einnig ber […][236].</u>[237] Slíkt verklag er einnig í samræmi við ISO 27001-vottun [birgis og þjónustuveitanda Símans][238].*

(108) Svo segir í bréfinu að:

> *Þá skal sérstaklega vakin athygli á því að aðgangur [birgis og þjónustuveitanda Símans][239] að kerfum Símans, […][240], er bæði eðlilegur og nauðsynlegur til að uppfylla skilyrði samningsins, t.d. til að geta samtengt raunumhverfi við uppfærslu þegar þau eru keyrð saman, en einnig til að uppfylla skilyrði laga um öryggi og virkni fjarskiptanetsins.*

---

[223] Hluti ákvörðunar ekki birtur opinberlega.
[224] Hluti ákvörðunar ekki birtur opinberlega.
[225] Hluti ákvörðunar ekki birtur opinberlega.
[226] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[227] Hluti ákvörðunar ekki birtur opinberlega.
[228] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[229] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[230] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[231] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[232] Hluti bréfs ekki birtur opinberlega.
[233] Hluti bréfs ekki birtur opinberlega.
[234] Undirstrikun Fjarskiptastofu.
[235] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[236] Hluti bréfs ekki birtur opinberlega.
[237] Undirstrikun Fjarskiptastofu.
[238] Nafn birgis og þjónustuveitanda Símans er ekki birt opinberlega.
[239] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[240] Hluti bréfs ekki birtur opinberlega.

Þá er nauðsynlegt að mati Símans að aðgangur [birgis og þjónustuveitanda Símans][241] sé […][242] [243] til þess að geta greint frávikið, brugðist við og gert viðeigandi úrbætur, eftir því sem þörf krefur hverju sinni. […][244], gefur það augaleið að það myndi fela í sér verulega áhættu fyrir Símann […][245]. Eins og skoðun FST gefur til kynna er ljóst að hver mínúta sem líður á meðan á atviki stendur getur skipt sköpum […][246].[247]

(109) Með bréfi Fjarskiptastofu, dags. 10. ágúst 2023, óskaði stofnunin svo eftir upplýsingum um hvernig aðgangsheimildum að kerfum Símans fyrir [birgi og þjónustuveitanda Símans][248] var háttað fyrir umrætt öryggisatvik. Í svari Símans, dags. 11. september 2023, segir m.a. að:

Að því sögðu skal þó aftur tekið fram að […][249], en Síminn minntist á það í svarbréfi félagsins, dags. 23. maí 2022. Hefur Síminn tekið saman gögn sem skýra nánar umræddu kerfi, þ.e. gögn frá [birgi og þjónustuveitanda Símans][250], sem fylgja með svarbréfi þessu.

(110) Af framangreindu er því ljóst að [birgir og þjónustuveitandi Símans][251] hafði […][252] aðgang að þeim kerfum Símans sem voru andlag umrædds þjónustusamnings […][253] og var félaginu […][254] að umræddum fjarskiptanetum Símans.

(111) Síminn virðist því […][255]. Að því sögðu skal þó tekið fram að Fjarskiptastofa gerir ekki athugasemdir við það að ríkt samstarf geti verið milli fjarskiptafyrirtækja og birgja.

(112) Til þess ber að líta að aðgangsstýring er almenn öryggisráðstöfun til að lágmarka áhættu á óheimiliðum aðgerðum og mistökum, þ.e.a.s. vönduð aðgangstýring er hluti af áhættustýringu fjarskiptafyrirtækja. Í þessu samhengi ber einnig að líta til þess að aðgangstýring telst til áhættustýringar skv. m.a. lið A.9 viðauka staðalsins ISO 27001, sbr. grein 6.1.3 c).

(113) Í kjölfar umrædds öryggisatviks þá rannsakaði [birgir og þjónustuveitandi Símans][256] umrætt öryggisatvik. Í frávikaskýrslu [birgis og þjónustuveitanda Símans], dags. 17. desember 2021, er öryggisatvikinu lýst og áhrifum þess, orsakir greindar og þeim úrbótaraðgerðum lýst

[241] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[242] Hluti bréfs ekki birtur opinberlega.
[243] Undirstrikun Fjarskiptastofu.
[244] Hluti bréfs ekki birtur opinberlega.
[245] Hluti bréfs ekki birtur opinberlega.
[246] Hluti bréfs ekki birtur opinberlega.
[247] Undirstrikun Fjarskiptastofu.
[248] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[249] Hluti bréfs ekki birtur opinberlega.
[250] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[251] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[252] Hluti ákvörðunar ekki birt opinberlega.
[253] Hluti ákvörðunar ekki birt opinberlega.
[254] Hluti ákvörðunar ekki birt opinberlega.
[255] Hluti ákvörðunar ekki birt opinberlega.
[256] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

sem ætlað var að koma í veg fyrir að svipuð atvik endurtaki sig. Ein þessara aðgerða var að […][257]. En í skýrslunni segir:

> *More strictly guidelines/process for […][258] and including a clearly […][259] for the work to be executed during the […][260].*

(114) Einnig er talað um að verkaðferð verði bætt, samskipti aðila verði stöðug á meðan breytingar eiga sér stað […][261].

(115) Ákvæði 12. gr. reglna nr. 1221/2007 kveður á um skipulagslegar- og tæknilegar ráðstafanir sem fjarskiptafyrirtæki skulu viðhafa til að verja almenn fjarskiptanet sín. Í því skyni skuli fyrirtækin m.a. nota aðgangsheimildir, aðgangstýringu og óhrekjanleika, og takmarka aðgang starfsmanna að upplýsingum við þær sem eru þeim nauðsynlegar til að þeir geti sinnt starfi sínu, og við þann tíma sem nauðsynlegur er.

(116) Eins og fram hefur komið þá var umræddur starfsmaður [birgis og þjónustuveitanda Símans][262] að vinna í því að vandræðaveiða (troubleshooting) til að kanna hvort uppfærslan í […][263] hefði heppnast þegar meint öryggisatvik átti sér stað. Af frávikaskýrslu [birgis og þjónustuveitanda Símans] verður ekki komist að annarri niðurstöðu en að […][264] og að það hafi verið ein orsök umrædds öryggisatviks. Af framangreindu er því ljóst að ekki var með fullnægjandi hætti takmarkaður aðgangur umrædds starfsmanns [birgis og þjónustuveitanda Símans][265] að upplýsingum við þær sem honum var nauðsynlegt til að hann gæti sinnt starfi sínu, […][266]. En slíkt er ekki í samræmi við kröfur 6. tl. 12. gr. reglna nr. 1221/2007.

(117) Þar sem áhættustýringu verður ekki útvistað skv. 2. málsl. 13. gr. reglna nr. 1221/2007 þá verður ekki komist að annarri niðurstöðu en þær skyldur sem leiða af ákvæði 6. tl. 12. gr. reglna nr. 1221/2007 hvíli á Símanum og því hafi félagið brotið gegn þeim kröfum sem ákvæðið kveður á um, með því að gera ekki fullnægjandi ráðstafanir til að takmarka aðgang umrædds starfsmanns að upplýsingum við þær sem honum var nauðsynlegar til að hann gæti sinnt starfi sínu þegar öryggisatvikið átti sér stað.

Hlítni við verklagsreglur um breytingar

(118) Í gagnabeiðni Fjarskiptastofu, dags. 10. ágúst 2023, óskaði stofnunin eftir lýsingu á því hvernig Síminn tryggði að verktaki félagsins (starfsfólk [birgis og þjónustuveitanda Símans][267]) færu að verklagsreglum Símans við framkvæmd breytinga. Í svarbréfi Símans, dags. 11. september 2023, segir eftirfarandi:

257 Hluti ákvörðunar ekki birt opinberlega.
258 Hluti skýrslunnar ekki birt opinberlega.
259 Hluti skýrslunnar ekki birt opinberlega.
260 Hluti skýrslunnar ekki birt opinberlega.
261 Hluti ákvörðunar ekki birt opinberlega.
262 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
263 Hluti ákvörðunar ekki birt opinberlega.
264 Hluti ákvörðunar ekki birt opinberlega.
265 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
266 Hluti ákvörðunar ekki birt opinberlega.
267 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

Síminn gerir ekki þá kröfu í þjónustusamningi við […][268].

(119) Af svörum Símans verður ekki annað ráðið en eða Síminn gerði ekki þá kröfur til [birgis og þjónustuveitanda Símans][269] að félagið hlíti verklagsreglum félagsins við framkvæmd breytinga. […][270].

(120) Við skoðun á þeim verklagsreglum Símans sem í gildi voru þegar umrætt öryggisatvik átti sér stað sbr. framlagt skjal „[…][271]", segir hins vegar eftirfarandi:

Verklagsregla um breytingarstjórnun nær til allra upplýsinga- og fjarskiptakerfa Símans ásamt þeirra kerfa sem Síminn hefur samið um útvistun á til samstarfsaðila[272].

(121) Verklagsreglur um breytingastjórnun Símans áttu því að gilda um þær breytingar sem [birgir og þjónustuveitandi Símans][273] var að vinna að fyrir Símann þar sem félagið hafði samið við [birgi og þjónustuveitanda Símans][274] um að annast rekstur fjarskiptaneta sinna að hluta. Af framangreindu leiðir því að Síminn fór ekki eftir sínum eigin verklagsreglum við framkvæmd umræddra breytinga þar sem félagið […][275]. Það að Síminn fari ekki eftir sínum eigin verklagsreglum við framkvæmd breytinga felur í sér að þær eru ekki framkvæmdar þannig að þær trufli sem minnst fjarskiptaþjónustu og er slíkt ekki í samræmi við kröfur 2. mgr. 23. gr. reglna nr. 1222/2007.

Prófanir

(122) Með bréfi Fjarskiptastofu, dags. 6. maí 2022, var spurt hvort fyrirhugaðar breytingar á kjarnakerfum Símans væru prófaðar áður en þær væru keyrðar í raunumhverfi og hvort gerðar væru áætlanir um prófanir á kjarnakerfum félagsins. Síminn svaraði því játandi í svarbréfi, dags. 23. maí 2022. Í bréfi Fjarskiptastofu, dags. 10. ágúst sl. 2023, óskaði svo stofnunin eftir afriti þeirra prófana sem fram fóru áður en framkvæmdar voru þær breytingar í kerfum Símans sem ollu umræddu öryggisatviki. Síminn svaraði því til í svarbréfi sínu, dags. 11. september 2023, að:

Á þeim tímapunkti sem atvikið á sér stað er verkefnið á lokastigum, þ.e. verið var að undirbúa samkeyrslu kerfanna á nýjan leik að lokinni uppfærslu. Mistök af þessum toga er ekki hægt að prófa fyrirfram, og því augljóst að slíkar prófanir eru og voru ekki gerðar[276].

(123) Ekki er hægt að skilja svar Símans við skýrri spurningunni stofnunarinnar með öðrum hætti en að engar prófanir hafi farið fram áður en þær breytingar í kerfum Símans sem ollu

[268] Hluti bréfs ekki birt opinberlega.
[269] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[270] Hluti ákvörðunar ekki birt opinberlega.
[271] Heiti skjals ekki birt opinberlega.
[272] Undirstrikun Fjarskiptastofu.
[273] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[274] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[275] Hluti ákvörðunar ekki birt opinberlega.
[276] Undirstrikun Fjarskiptastofu.

umræddu öryggisatviki voru framkvæmdar. En um var að ræða […][277] uppfærsla úr […][278]. Félagið hefur ekki getað afhent nein gögn er styðja það að prófanir hafi farið fram áður en til breytinganna kom og neitaði að svo hafi verið gert í síðara svari sínu. En slíkt er ekki í samræmi við kröfur sem gerðar eru til áhættustýringar skv. liðum A.14.2.8 og A.2.9 staðalsins ISO 27001 og grein 12.1.2 staðalsins ÍST EN ISO/IEC 27002:2017[279] (hér eftir ISO 27002).

Yfirsýn og stjórnun breytinga

(124) Með vísan til alls framangreind er það mat Fjarskiptastofu að Síminn hafi skort yfirsýn yfir framkvæmd umræddrar breytingar þar sem ekki var rétt staðið að útvistun reksturs fjarskiptanets Símans til [birgis og þjónustuveitanda Símans][280] í þjónustusamningi og samþykkt breytingabeiðni bæði óskýr og innihaldslítil auk þess sem verkferlar um framkvæmd breytinga voru ófullnægjandi. Það er einnig mat Fjarskiptastofu að framkvæmd umræddrar breytingar þann 12. október 2021 hafi ekki heldur verið stýrt með fullnægjandi hætti af Símanum þar sem aðgangsstýring var ófullnægjandi auk þess sem ekki var farið að verklagsreglum um framkvæmd breytinga og engar prófanir fóru fram áður en umræddar breytingar voru framkvæmdar. Af öllu framangreindu leiðir að umrædd breyting var ekki framkvæmd þannig að hún truflaði sem minnst fjarskiptaþjónustu Símans en slíkt er ekki í samræmi við kröfur 2. mgr. 23. gr. reglna nr. 1222/2007.

<u>Varabúnaður</u>

(125) Í frávikaskýrslu Símans kemur fram að farsímakjarni Símans […][281]. Samkvæmt bréfi Símans, dags. 11. september 2023, segir að *„[…][282]“*. Af því leiðir að undir venjulegum kringumstæðum eru farsímakjarnar Símans […][283] varabúnaður […][284].

(126) Samkvæmt verkáætlun fyrir umræddar breytingar (mynd 6) kemur fram að meðan verið var að uppfæra farsímakjarna Símans […][285] þá var áætlað að […][286] í 7 vikur. Síðan er gert ráð fyrir því í verkáætluninni að meðan uppfærsla fari fram […][287] í aðrar 7 vikur. Þannig að á a.m.k. 14 vikna tímabili, skv. verkáætlun, er áætlað […][288]. Í bréfi Símans, dag. 11. september 2023, segir eftirfarandi:

> *Þegar atvikið á sér stað er uppfærslum lokið á öllum kerfunum […][289] [290] og á þeim tímapunkti er búið að samtengja kerfin, þó svo að kerfin […][291] hafi ekki verið byrjuð að*

---

[277] Hluti ákvörðunar ekki birt opinberlega.
[278] Hluti ákvörðunar ekki birt opinberlega.
[279] Sú útgáfu staðalsins sem var í gildi þegar atvik máls áttu sér stað.
[280] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[281] Hluti ákvörðunar ekki birt opinberlega.
[282] Hluti bréfs ekki birt opinberlega.
[283] Hluti ákvörðunar ekki birt opinberlega.
[284] Hluti ákvörðunar ekki birt opinberlega.
[285] Hluti ákvörðunar ekki birt opinberlega.
[286] Hluti ákvörðunar ekki birt opinberlega.
[287] Hluti ákvörðunar ekki birt opinberlega.
[288] Hluti ákvörðunar ekki birt opinberlega.
[289] Hluti verkáætlunar ekki birt opinberlega.
[290] Með tölvubréfi, dags. 8. nóvember 2023, staðfesti Síminn að hér væri átt við […].
[291] Hluti verkáætlunar ekki birt opinberlega.

taka umferð. Þessi fasi uppfærslunnar, þ.e. að taka eitt og eitt hugbúnaðarkerfi […][292] í notkun, er gert yfir nokkurra daga tímabil.

(127) Svo segir í bréfinu:

Eins og segir hér ofar í skýringum félagsins við spurningu 5, þá var verið að undirbúa það að taka […][293] í notkun, enda uppfærslum lokið, og samtenging komin á milli kjarnanna þó svo að […][294] væri ekki að afgreiða umferð[295], þ.e. „óvirkur".

(128) Af gögnum málsins er því ljóst að þegar umrætt öryggisatvik á sér stað er verið var að undirbúa samkeyrslu kerfanna á nýjan leik að uppfærslu lokinni í […][296] og að tenging er kominn á milli farsímakjarnanna. Samkvæmt verkáætlun náði þessi verkþáttur yfir tímabilið frá 11. – 15. október 2021.

(129) Í boðaðri ákvörðun Fjarskiptastofu, dags. 5. janúar 2023, taldi stofnunin að enginn varabúnaður hefði verið til staðar á 14 vikna tímabili meðan uppfærslan fór fram, þar sem […][297] voru í uppfærslu á umræddu tímabili. Síminn mótmælti þeirri staðhæfingu í andmælabréfi, dags. 15. febrúar 2023, en þar segir m.a:

Eins og áður segir er Síminn með […][298] þar sem kjarnakerfi félagsins er staðsett, þ.e. […][299]. […][300] með varabúnað ef búnaðurinn bilar, […][301] með fullnægjandi varabúnað[302]. Búnaður […][303] gat bilað án þess að slíkt hefði áhrif á uppitíma þjónustunnar af þeirri ástæðu að innbyggt í kerfið er að ef einn tölvubúnaður myndi bila þá tæki annar tölvubúnaður við.

(130) Með framangreindum ummælum Símans í andmælabréfinu komu fram nýjar upplýsingar í málinu, þ.e. að hver farsímakjarni Símans hefði sinn eigin varabúnað. Fjarskiptastofa óskaði því eftir nánari upplýsingum um varabúnað Símans í bréfi, dags. 10. ágúst 2023. Var Síminn m.a. spurður hvers vegna varabúnaðurinn […][304] virkuðu ekki þegar umrætt öryggisatvik átti sér stað. Þessari spurningu var ekki svarað af hálfu Símans heldur einungis sagt að það sem fram kom í andmælabréfinu varðandi það að búnaður hafi „bilað" hafi ekki verið rétt, þ.e. að enginn búnaður hefði bilað *„heldur var slökkt á röngum búnaði sökum mannlegra mistaka.".*

---

[292] Hluti verkáætlunar ekki birt opinberlega.
[293] Hluti bréfs ekki birt opinberlega.
[294] Hluti bréfs ekki birt opinberlega.
[295] Undirstrikun Fjarskiptastofu.
[296] Hluti ákvörðunar ekki birt opinberlega.
[297] Hluti ákvörðunar ekki birt opinberlega.
[298] Hluti bréfs ekki birt opinberlega.
[299] Hluti bréfs ekki birt opinberlega.
[300] Hluti bréfs ekki birt opinberlega.
[301] Hluti bréfs ekki birt opinberlega.
[302] Undirstrikun Fjarskiptastofu.
[303] Hluti bréfs ekki birt opinberlega.
[304] Hluti ákvörðunar ekki birt opinberlega.

(131) Í bréfi Fjarskiptastofu, dags. 10. ágúst 2023, spurði stofnunin einnig um það hvaða varabúnað og önnur úrræði Síminn notaðist við til að viðhalda samfelldum rekstri. Í svarbréfi Símans, dags. 11. september 2023, sagði þetta um varabúnað Símans:

[…][305]

(132) Samkvæmt þessu er ljóst að undir venjulegum kringumstæðum eru farsímakjarnar Símans í […][306] varabúnaður […][307]. Einnig kemur þar fram að búnaður á hverju stað samanstendur af […][308] og getur farsímakjarninn á hverju stað starfað án þess að til þjónustuskerðingar komi […][309].

(133) Af gögnum málsins er ljóst að á meðan umrædd uppfærsla á farsímakerfi Símans átt sér stað þá gat […][310] ekki verið varakerfi fyrir […][311], þar sem gert var ráð fyrir því að uppfærsla færi fram í […][312] á um 14 vikna tímabili, skv. verkáætlun, […][313]. Síminn hefur haldið því fram að þó áætlað væri að […][314] hafi verið í uppfærslu […][315] á 14 vikna tímabili hafi samt sem áður verið gert ráð fyrir fullnægjandi varabúnað á þessu tímabili þar sem hver farsímakjarni fyrir sig hafi sinn eigin varabúnað. Síminn hefur hins vegar ekki getað útskýrt það með fullnægjandi hætti hvernig slíkur varabúnaður á hverju stað fyrir sig myndi hafa átt að virka til að koma í veg fyrir umrætt útfall og hvers vegna hann virkað ekki þegar það átti sér stað.

(134) Ljóst er af svörum Símans, dags. 27. desember 2021, og frávikaskýrslu [birgis og þjónustuveitanda Símans][316] að umrætt öryggisatvik fólst í því að hluti af farsímakjarna Símans missti samband við aðrar kerfiseiningar sem svo olli afgerandi truflunum á talþjónustu yfir 3G og 2G. Náði truflunin til allt að 150.000 notenda í 32 mínútur. Að auki hafði þessi bilun áhrif á hluta fastlínukerfa Símans þar sem númeraflutningsuppfletting er sameiginleg með farsíma og talsíma í kerfum Símans. Áætlað var að um 50% af fastlínu uppköllum á þessu tímabili hafi einnig orðið fyrir áhrifum og að niðritími hafi verið um 30 mínútur.

(135) Þar sem umfang öryggisatviksins var með þeim hætti sem að framan er lýst er því ljóst að fullnægjandi varabúnaður var ekki til staðar þegar það gerðist. Engu skiptir í því samhengi þó Síminn segi að slíkur búnaður hafi verið til staðar, þ.m.t. varabúnaður fyrir hvorn kjarna fyrir sig, því augljóst er að jafnvel þó slíkur varabúnaður hafi verið til staðar þá virkaði hann ekki þegar á reyndi, sem jafna má til þess að ekki var nægur varabúnaður og önnur úrræði til staðar til að viðhalda samfelldum rekstri.

305 Hluti bréfs ekki birt opinberlega.
306 Hluti ákvörðunar ekki birt opinberlega.
307 Hluti ákvörðunar ekki birt opinberlega.
308 Hluti ákvörðunar ekki birt opinberlega.
309 Hluti ákvörðunar ekki birt opinberlega.
310 Hluti ákvörðunar ekki birt opinberlega.
311 Hluti ákvörðunar ekki birt opinberlega.
312 Hluti ákvörðunar ekki birt opinberlega.
313 Hluti ákvörðunar ekki birt opinberlega.
314 Hluti ákvörðunar ekki birt opinberlega.
315 Hluti ákvörðunar ekki birt opinberlega.
316 Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

(136) Eins og fram hefur komið þá átti öryggisatvikið sér stað þegar tenging var kominn milli farsímakjarna Símans […][317] og verið var að undirbúa samkeyrslu […][318]. En til þess ber að líta að hér var um mjög áhættusaman hluta uppfærslunnar að ræða þar sem tenging var kominn milli farsímakjarnanna, en umrætt öryggisatvik gerðist einmitt við þennan verkþátt. Af öllu framangreindu er ljóst að ekki var til staðar nægur varabúnaður og önnur úrræði til að viðhalda samfelldum rekstri þegar unnið var að umræddum breytingum 12. október 2021, en slíkt er ekki í samræmi við kröfur 4. mgr. 20. gr. reglna nr. 1222/2007.

4.4.3 Neyðaráætlun

<u>Innihald áætlunarinnar</u>

(137) Eins og fram hefur komið þá átti umrætt öryggisatvik sér stað um miðjan dag kl. 11:30 þann 12. október 2021 og olli útfalli á þjónustu Símans sem stóð yfir í um 32 mínútur. Í svörum Símans, dags. 11. september 2023, kemur fram að neyðaráætlun var virkjuð kl. 11:54 sama dag. Þannig er ljóst að neyðaráætlun var virkjuð töluvert eftir að umrætt öryggisatvik átti sér stað. Hins vegar ber að líta til þess að þegar upp komst um útfallið var brugðist hratt við enda tók endurreisn skamman tíma.

(138) Fjarskiptastofa óskaði eftir neyðaráætlun Símans með bréfi, dags. 6. maí 2022. Þann 24. maí 2022 var stofnuninni afhent skjalið „[…][319]“, en í svarbréfi Símans er vakin athygli á því að um er að ræða neyðaráætlun Símans þrátt fyrir að heitið sé […][320].

(139) Við skoðun á neyðaráætlun Símans sést að til staðar eru í kerfinu […][321] listar yfir birgja og tengiliði og gátlisti viðbragðshóps. Í skjalinu er einnig sérstakur kafli um hlutverk og ábyrgð viðbragðshópa sem eiga að koma saman í svokölluðu […][322]. Í áætluninni kemur einnig fram að samskipti við viðbragðshópana fari í gegnum […][323]. Þá er þar einnig að finna tengla á viðbragðs- og endurheimtuáætlanir sem og birgja- og tengiliðalista.

(140) Við skoðun Fjarskiptastofu á umræddri neyðaráætlun kom þó í ljós að ekki var þar að finna lýsingu á viðhaldi handbóka fyrir daglegan rekstur búnaðar. En skv. 2. tl. 8. gr. reglna nr. 1222/2007 á slík lýsing að koma fram í neyðaráætlun. Með bréfi Fjarskiptastofu, dags. 10. ágúst 2023, óskað stofnunin eftir afriti af verklagsreglum félagsins, sem í gildi var þann 12. október 2021, þar sem er að finna lýsingu á viðhaldi handbóka fyrir daglegan rekstur búnaðar.

(141) Í bréfi Símans, dags. 11. september 2023, er framangreindri spurningu svarað með eftirfarandi hætti:

---

[317] Hluti ákvörðunar ekki birt opinberlega.
[318] Hluti ákvörðunar ekki birt opinberlega.
[319] Heiti skjals ekki birt opinberlega.
[320] Hluti ákvörðunar ekki birt opinberlega.
[321] Hluti ákvörðunar ekki birt opinberlega.
[322] Hluti ákvörðunar ekki birt opinberlega.
[323] Hluti ákvörðunar ekki birt opinberlega.

Hvernig skal unnið með farsímakjarna frá [birgi og þjónustuveitanda Símans][324] er að finna í […][325], kallað […][326], sem er hýst hjá Símanum, sbr. skjáskot hér neðar.

(142) Með bréfinu fylgi svo skjáskot af yfirlitssíðu af […][327], en þar kom ekki fram lýsing á viðhaldi handbóka fyrir daglegan rekstur búnaðar.

(143) Við skoðun Fjarskiptastofu á umræddri neyðaráætlun kom svo einnig í ljós að ekki var þar að finna skilgreiningu á hámarkstíma rekstrarstöðvunar áður en gripið er til áætlunarinnar. En skv. 4. tl. 8. gr. reglna nr. 1222/2007 á að skilgreina hámarkstíma rekstrarstöðvunar áður en gripið er til neyðaráætlunar. Með bréfi Fjarskiptastofu, dags. 10. ágúst 2023, óskaði stofnunin því eftir afriti af verklagsreglum félagsins, sem í gildi voru þann 12. október 2021, þar sem skilgreindur er leyfilegur hámarks niðritími kerfa áður en gripið er til neyðaráætlunar. Í svarbréfi Símans, dags. 11. september 2023, kemur fram eftirfarandi afstaða félagsins:

Síminn vekur athygli á að samkvæmt umræddu ákvæði í reglum nr. 1222/2007 er talað um „rekstrarstöðvun", en ekki „niðritíma" kerfa.

Mikill munur er á því hvort um sé að ræða „niðritíma" á kerfi annars vegar, sem öll félög eiga við í rekstri sínum, eða „rekstrarstöðvun" hins vegar. Hið síðarnefnda felur í sér allsherjar stöðvun á rekstri þjónustunnar, sem átti sér ekki stað í þessu tilviki.

(144) Afstaða Símans er því sú að umrædd skilgreining í neyðaráætlun á hámarkstíma rekstrarstöðvunar áður en gripið er til áætlunarinnar, sbr. 4. tl. 8. gr., eigi einungis við um allsherjar stöðvunar á rekstri þjónustu. Skv. 8. gr. reglna nr. 1222/2007 skulu gerðar ráðstafanir til að tryggja samfelldan og órofinn rekstur almennra fjarskiptaneta og fjarskiptaþjónustu. Í því skyni skulu fjarskiptafyrirtæki setja sér skriflega neyðaráætlun, sem byggir á niðurstöðum áhættumats. Í samræmi við það skal lýsa áætlun um ráðstafanir til að endurræsa óvirk fjarskiptanet og mögulega endurheimta upplýsingar sem kunna að hafa misfarist eða skemmst. Felur neyðaráætlun því í sér lýsingu á ráðstöfunum til að endurræsa óvirk fjarskiptanet og mögulega endurheimta upplýsingar sem kunna að hafa misfarist eða skemmst. Af því leiðir að ef fjarskiptanet verða óvirk ber fjarskiptafyrirtæki að virkja neyðaráætlun og þarf því ekki að vera um alherjar stöðvun á rekstri þjónustu að ræða til að svo sé. Það er því mat Fjarskiptastofu að með hugtakinu „rekstrarstöðvun" í framangreindu ákvæði sé því ekki átt við allsherjar stöðvunar á rekstri þjónustu, heldur miðist umfang umrædds hugtaks við það hvort tilefni er til að virkja neyðaráætlun í skilningi 8. gr. reglnanna.

(145) Í svarbréfi Símans, dags. 11. september 2023, kemur einnig fram að:

Síminn er með verklagsreglu sem tekur á rekstraratvikum, og ber heitið „[…][328]", sem þegar hefur verið afhent FST og hefur áður verið bent á að sé verið að yfirfara og uppfæra um þessar mundir. <u>Meðal þess sem skoðað er er að bæta þar einnig við umfjöllun um</u>

[324] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[325] Hluti bréfs ekki birt opinberlega.
[326] Hluti bréfs ekki birt opinberlega.
[327] Hluti ákvörðunar ekki birt opinberlega.
[328] Hluti bréfs ekki birt opinberlega.

„rekstrarstöðvun", í skilningi 4. tl. 8. gr. reglna nr. 1222/2007[329]*, þótt slíkar breytingar væru með öllu ótengdar því atviki sem hér er til umfjöllunar.*

(146) Samkvæmt svari Símans var því ekki í neyðaráætlun félagsins skilgreining á hámarkstíma rekstrarstöðvunar áður en gripið er til áætlunarinnar.

(147) Af öllu framangreind leiðir að þegar umrædd öryggisatvik átti sér stað kom ekki fram í neyðaráætlun Símans, lýsing á viðhaldi handbóka fyrir daglegan rekstur búnaðar eða skilgreining á hámarkstíma rekstrarstöðvunar áður en gripið er til áætlunarinnar. En slíkt er ekki í samræmi við þær kröfur sem fram koma í 2. og 4. tl. 8. gr. reglna nr. 1222/2007.

Prófun neyðaráætlunar

(148) Í bréfi Fjarskiptastofu, dags. 6. maí 2022, óskaði stofnuninn eftir afriti af síðustu þremur prófunum á neyðaráætlun og niðurstöðum þeirra. Í svarbréfi Símans, dags. 23. maí 2022, bárust skjámyndir af þremur raunverulegum atvikum sem áttu sér stað 2019, 2020 og 2021. En þar kom fram að Síminn hafði farið yfir viðkomandi atvik sem prófun á neyðaráætlun og lagt mat á það hvernig til tókst og lagðar til úrbætur ef svo bar undir. Kom þar einnig fram að um væri að ræða kröfur skv. lið 9.2 í staðlinum ISO 27001 varðandi innri úttekt og um að ræða stýringu skv. lið 17.1.3 staðalsins ISO 27002 varðandi sannprófun, rýni og mat á samfelldu upplýsingaröryggi[330]. Einnig kom fram í framangreindum skjámyndum Símans að verið var að gæta hlítingu við m.a. reglur nr. 1222/2007 og staðalinn ISO 27001.

(149) Reglur nr. 1221/2007 og 1222/2007 fjalla um stjórnkerfi upplýsingaröryggis og að því leyti sem ákvæði reglnanna fjalla um það verður að skýra þau til samræmis við þau ákvæði staðalsins ISO 27001 er varðar stjórnkerfi upplýsingaröryggis, sbr. 3. mgr. 2. gr. reglna nr. 1221/2007 og 3. málsl. 4. gr. reglna nr. 1222/2007. Enda kveða ákvæði 3. mgr. 2. gr. reglna nr. 1221/2007 og 3. málsl. 4. gr. reglna nr. 1222/2007 á um það að til hliðsjónar megi styðjast við staðalinn ISO 27001 þegar kemur að hlítingu við ákvæði reglnanna. Skv. gögnum málsins hefur Síminn verið með ISO 27001 vottun fyrir stjórnkerfi upplýsingaöryggis síðan 12. maí 2016.

(150) Í lið A.17.1 staðalsins ISO 27001 er kveðið á um samfellt upplýsingaröryggi sem varðar neyðaráætlun þeirra skipulagsheilda sem fara að staðlinum og m.a. hvernig slík áætlun er prófuð. En skv. lið A.17.1.1 við staðalinn þá skal skipulagsheild ákvarða kröfur sínar varðandi upplýsingaöryggi og samfellda stjórnun á upplýsingaöryggi við erfiðar aðstæður, t.d. í hættuástandi eða við áfall. Svo er kveðið á um það í lið A.17.1.2 að skipulagsheildin skuli koma á, skjalfesta, innleiða og viðhalda ferlum, verklagsreglum og stýringum til að tryggja það stig samfellds upplýsingaöryggis sem krafist er við erfiðar aðstæður. Að lokum er svo kveðið á um það í lið A.17.1.3 að skipulagsheildin skuli *sannprófa settar og innleiddar stýringar fyrir samfellt upplýsingaöryggi með reglulegu millibili til þess að tryggja að þær séu gildar og markvirkar við erfiðar aðstæður*. Framangreind ákvæði staðalsins eru samsvarandi ákvæði 8. gr. reglna nr. 1222/2007 er varðar neyðaráætlun eða ráðstafanir til að tryggja samfelldan og órofinn rekstur almennra fjarskiptaneta og fjarskiptaþjónustu, þ.m.t. kröfur um að neyðaráætlun sé prófuð reglulega til að til að tryggja virkni hennar.

[329] Undirstrikun Fjarskiptastofu.
[330] Sjá bls. 16 í staðlinum ÍST EN ISO/IEC 27002:2017.

(151) Í lið A.16.1 staðalsins ISO 27001 er svo kveðið á um stjórnun á upplýsingaröryggisatvikum og umbótum. En liður A.16.1.4 kveður á um það að meta skuli upplýsingaöryggisatburði og ákveða hvort þeir skuli flokkaðir sem upplýsingaöryggisatvik. Svo er kveðið á um það í lið A.16.1.6 *að nota skuli þekkingu sem fæst með því að greina og leysa úr upplýsingaöryggisatvikum til þess að draga úr líkum á eða áhrifum af atvikum í framtíðinni*. Þess skal getið að þau þrjú atvik sem fram komu í skjáskoti svarbréfs Símans myndu öll teljast til upplýsingaröryggisatviks í skilningi staðalsins, sbr. grein 3.31 staðalsins ÍST EN ISO/IEC 27000:2018, enda var neyðaráætlun virkjuð í öllu tilvikum, þótt ekki hafi verið um rekstrarstöðvun allrar þjónustu í skilningi Símans að ræða. En eitt atvikið varðaði […][331] sem hafði áhrif á sjónvarpsþjónustu Símans, eitt atvikið varðaði rafmagnsleysi í […][332] og að lokum varðaði eitt tilvikið atvik í farsímakjarnanum í […][333] sem hafði áhrif á um helming farsímanotenda. En þar var atvikunum lýst og lagt mat á það hvernig til tókst með viðbrögð við þeim og lagðar til úrbætur ef svo bar undir. Slík atvikameðhöndlun telst til hluta af greiningu og úrlausn á upplýsingaöryggisatvikum í því skyni að draga úr líkum á eða áhrifum af atvikum í framtíðinni í skilningi liðar A.16.1.6 þar sem um er að ræða rannsókn eða úttekt á viðbrögðum við atvikum.

(152) Af framangreindu leiðir að rannsókn eða úttekt á atvikum skv. lið A.16.1.6 og prófun neyðaráætlunar skv. lið A.17.1.3 eru tvenn aðskilin fyrirbæri í staðlinum ISO 27001. Það er mat Fjarskiptastofu að þær úttektir sem fram komu í skjáskoti svarbréfs Símans, teljast til hluta rannsóknar eða úttektar á upplýsingaröryggisatviks í skilningi liðar A.16.1.16 staðalsins ISO 27001, en ekki prófunar neyðaráætlunar í skilningi liðar A.17.1.3. En í umræddum tilvikum var verið að meta hvernig til tókst með viðbrögð við raunverulegum atvikum og lagðar til úrbætur ef svo bar undir, en ekki er verið að prófa eða æfa neyðaráætlun til að tryggja virkni hennar. En eðli máls samkvæmt er ekki hægt að prófa viðbrögð við einhverju sem þegar hefur gerst.

(153) Með bréfi Fjarskiptastofu, dags. 10. ágúst 2023, óskaði stofnunin eftir síðustu þrem prófunum Símans á neyðaráætlun fyrir 12. október 2021, þar sem beitt var ímynduðum atvikum við prófanir á neyðaráætlun, þ.m.t. afrit af handritum æfinganna (prófananna), niðurstaða þeirra og hvort gripið var til úrbóta á grundvelli þeirra. Í svari Símans, dags. 11. september 2023, segir að:

> *Afrit af síðustu úttekt á ímynduðum atvikum fór fram árið 2018. Aðrar úttektir um ímynduð atvik hafa ekki farið fram síðan.*

(154) Með svarbréfinu var svo sent skjalið „[…][334]“, en þar kemur fram að 18. maí 2018 var haldin æfing á neyðaráætlun Símans og var tilgangur æfingarinnar að prófa ferla, samskipti og framgang aðgerða í neyð.

---

331 Hluti ákvörðunar ekki birt opinberlega.
332 Hluti ákvörðunar ekki birt opinberlega.
333 Hluti ákvörðunar ekki birt opinberlega.
334 Heiti skjals ekki birt opinberlega.

(155) Af öllu framangreindu er ljóst að umræddar úttektir á viðbrögðum við atvikum fela ekki í sér próf eða æfingu á neyðaráætlunar til að tryggja virkni hennar heldur rannsókn á viðbrögðum við raunverulegum atvikum. Einnig er ljóst að síðasta æfing Símans á neyðaráætlun átti sér stað 2018 og hefur Síminn ekki sýnt fram á að áætlunin hafi verið prófuð síðan til að tryggja virkni hennar. Skv. 8. gr. reglna nr. 1222/2007 skal prófa neyðaráætlun *reglulega* til að tryggja virkni hennar. Það að Síminn prófaði neyðaráætlun sína síðast með fullnægjandi hætti árið 2018 eða meira en þrem árum áður en atvik máls eiga sér stað getur ekki falið í sér að hún hafi verið prófuð reglulega, en slíkt er ekki í samræmi við þær kröfur sem fram koma í 8. gr. reglna nr. 1222/2007.

<u>Innra eftirlit</u>

(156) Í gagnabeiðni Fjarskiptastofu, dags. 6. maí 2022, var óskað eftir gildandi áætlun innra eftirlits. Síminn svaraði spurningunni með yfirliti úr verkefnastjórnunarkerfi sínu ([…][335]) (mynd 9).

[…][336]

Mynd 9: Myndin sýnir afrit af gildandi áætlun Símans um innra eftirlit. Myndin tiltekur fimm innri/ytri úttektir eða prófanir.

(157) Samkvæmt svörum Símans þá kemur í ljós að gildandi áætlun Símans um innra eftirlit félagsins vísar til rannsóknar á framangreindum atvikum sem áttu sér stað 2019, 2020 og 2021 sem Síminn telur vera prófanir á neyðaráætlun sinni. Af framangreindu er því ekki hægt að álykta annað en að Síminn telji sig með framangreindri úttekt eða rannsókn atvika vera að prófa neyðaráætlun og framkvæma innri úttekt í sömu andrá.

(158) Eins og að framan greinir þá kom fram í skjámyndum af þeim þremur raunverulegum atvikum sem rannsökuð voru, að um væri að ræða kröfur skv. grein 9.2 í staðalsins ISO 27001 varðandi innri úttekt, en sú grein er svohljóðandi:

> *Skipulagsheildin skal gera innri úttektir með fyrirfram ákveðnu millibili til þess að veita upplýsingar um hvort stjórnunarkerfið um upplýsingaöryggi:*
>
> *a) samræmist*
> *1) eigin kröfum skipulagsheildarinnar til stjórnunarkerfis síns um upplýsingaöryggi; og*
> *2) kröfum þessa alþjóðastaðals;*
> *b) sé innleitt með markvirkum hætti og því viðhaldið.*
>
> *Skipulagsheildin skal:*
> *c) skipuleggja, setja fram, innleiða og viðhalda úttektaráætlun(um), þ.m.t. um tíðni,*

[335] Hluti ákvörðunar ekki birt opinberlega.
[336] Yfirlit úr verkefnastjórnunarkerfi Símans ekki birt opinberlega.

aðferðir, ábyrgð, kröfur til skipulagningar og skýrslugjöf. Úttektaráætlanir skulu taka mið af mikilvægi ferlanna sem um ræðir og niðurstöðum fyrri úttekta;

d) skilgreina úttektarviðmið og umfang hverrar úttektar;
e) velja úttektarmenn og framkvæma úttektir sem tryggja óhlutdrægni og hlutleysi úttektarferlisins;
f) tryggja skýrslugjöf um niðurstöður úttektanna til viðeigandi stjórnenda; og
g) varðveita skjalfestar upplýsingar sem sönnunargögn um úttektaráætlanirnar og niðurstöður úttekta.

(159) Í grein 9.2 framangreinds staðals koma því fram mjög ríkar kröfur til framkvæmdar innri úttekta, m.a. er kveðið á um að velja skuli úttekarmenn og framkvæma skulu úttektir sem tryggja óhlutdrægni og hlutleysi úttektarferlisins. Sambærileg ákvæði er að finna í 8. gr. reglna nr. 1221/2007 og 9. gr. reglna nr. 1222/2007 varðandi innra eftirlit og verða þau að túlkast til samræmis við grein 9.2 staðalsins, sbr. 3. mgr. 2. gr. reglna nr. 1221/2007 og 3. málsl. 4. gr. reglna nr. 1222/2007.

(160) Eins og fram hefur komið þá er það mat Fjarskiptastofu að þær framangreindu úttektir eða rannsóknir á viðbrögðum við raunverulegum atvikum sem gildandi áætlun Símans um innra eftirlit félagsins vísar til og fram komu í skjáskoti svarbréfs Símans, dags. 23. maí 2022, teljist til rannsóknar upplýsingaöryggisatviks í skilningi liðar A.16.1.16 staðalsins ISO 27001. En slík rannsókn eða úttekt getur ekki falið í sér fullnægjandi innri úttekt skv. grein 9.2 framangreinds staðals, þar sem liður A.16.1.6 felur í sér áhættustýringu skv. grein 6.1.3 staðalsins og er aðgreind frá grein 9.2. En skv. staðlinum er gert ráð fyrir því að innri úttekt sé ekki hluti áhættustýringar heldur sé slíkri úttekt ætlað að taka út m.a. hvort áhættustýring skv. staðlinum sé fullnægjandi og er því grein 9.2 skýrlega aðskilin frá grein 6.1.3, sbr. viðauka A við staðalinn. Svo er í grein 9.2 gerðar aðrar og ríkari kröfur til úttekta líkt og fram hefur komið, m.a. til óhlutdrægni og hlutleysis ferlisins. Það að Síminn haldi því fram að rannsókn á viðbrögðum við raunverulegum atvikum teljist til krafna skv. grein 9.2 í umræddum staðli er því ekki samræmi við skýra aðgreiningu í staðlinum ISO 27001.

(161) Með bréfi, dags. 10. ágúst 2023, óskaði Fjarskiptastofa eftir upplýsingum um það hvort að sömu aðilar framkvæmdu prófanir á neyðaráætlun skv. 8. gr. reglna nr. 1222/2007 og viðhöfðu innra eftirlit til að tryggja virkni neyðaráætlunar skv. 9. gr. reglnanna fyrir 12. október 2021. Síminn svaraði framangreindri spurningu í svarbréfi, dags. 11. september 2023, þar sem m.a. kom fram að:

> *Varðandi framkvæmd innra eftirlits skv. 9. gr. sömu reglna hefur Síminn litið svo á að með áðurnefndum prófunum félagsins hafi það um leið uppfyllt skilyrði þessa ákvæðis, enda er bæði í 8. og 9. gr. reglnanna tilgreint sérstaklega að prófunin (8. gr.) og innra eftirlit (9. gr.) skuli framkvæma „til að tryggja virkni neyðaráætlunar". Það að prófa neyðaráætlun, eins og Síminn gerir, er um leið liður í innra eftirliti skv. 9. gr. Þá er hvergi vikið að því í umræddum ákvæðum að hér þurfi sinn hvor aðilinn að viðhafa tvenns konar innra eftirlit.*[337] *Engin ástæða er til að túlka reglurnar með svo þröngum hætti, m.t.t. markmiða 8. og 9. gr.*

[337] Undirstrikun Fjarskiptastofu.

(162) Í svari Símans kemur því skýrlega fram að félagið telur að hægt sé að framkvæma prófun á neyðaráætlun um leið og framkvæmt er innra eftirlit, þ.e. að hægt sé að gera þetta samtímis. Einnig verða svör Símans ekki skilin með öðrum hætti en að sömu aðilar framkvæmi meintar prófanir á neyðaráætlun og framkvæmi innra eftirlit.

(163) Eins og fram hefur komið er það mat Fjarskiptastofu að meint prófun neyðaráætlunar sé í raun rannsókn upplýsingaöryggisatviks í skilningi liðar A.16.1.16 staðalsins ISO 27001. Einnig er það mat Fjarskiptastofu að slík rannsókn eða úttekt sem Síminn framkvæmdi geti ekki falið í sér fullnægjandi innri úttekt skv. grein 9.2 framangreinds staðals þar sem liður A.16.1.6 felur í sér áhættustýringu, sbr. grein 6.1.3 staðalsins, en innri úttekt er ekki hlut áhættustýringar heldur ætlað að hafa eftirlit með að hún sé fullnægjandi. Einnig eru gerðar aðrar og ríkari kröfur til innri úttekta skv. grein 9.2 en gerðar eru til framkvæmdar áhættustýringar. En þær kröfur sem gerðar eru til innri úttekar skv. grein 9.2 er m.a. þær að velja skuli úttekarmenn og framkvæma skulu úttektir sem tryggja óhlutdrægni og hlutleysi úttektarferlisins. Það er því mat Fjarskiptastofu að sú tilhögun að sömu aðilar framkvæmi áhættustýringu skv. lið A.16.1.6 og framkvæmi innri úttekt með þeim hætti sem Síminn gerir sé ekki í samræmi við grein 9.2 þar sem ekki er hægt með því að tryggja óhlutdrægni og hlutleysi úttektarferlisins.

(164) Samkvæmt 8. gr. reglna nr. 1221/2007 og 9. gr. reglna nr. 1222/2007 skal framkvæma innra eftirlit kerfisbundið samkvæmt fyrir fram skilgreindri aðferð. Með bréfi, dags. 10. ágúst 2023, óskaði Fjarskiptastofa eftir afriti af skilgreindri aðferð Símans um kerfisbundna framkvæmd á innra eftirliti. Sem svar við þeirri spurningu var stofnuninni afhent skjalið „[…][338]“. Samkvæmt þeim verklagsreglum er gert ráð fyrir bæði sjálfvirku og handvirku eftirliti sem er hluti af skipulögðu eftirliti með frávikum í starfsemi Símans og er markmið þess að grípa frávik og leiðrétta þau sem fyrst til að tryggja öryggi upplýsinga og starfsmanna Símans. Hvergi í verklagsreglunum er þess getið að innra eftirlit feli í sér rannsókn eða úttekt á viðbrögðum við raunverulegum atvikum líkt og gildandi áætlun innra eftirlits Símans gerir ráð fyrir og ekki verður heldur séð hvernig slík rannsókn atvika samræmist markmiðum framangreindra reglna. Einnig er ekki getið í verklagsreglunum að velja skuli úttektarmenn og framkvæma úttektir sem tryggi óhlutdrægni og hlutleysi úttektarferlisins.

(165) Eins og fram hefur komið þá er það mat Fjarskiptastofu að það að rannsaka viðbrögð við raunverulegum atvikum feli í sér rannsókn upplýsingaöryggisatviks í skilningi liðar A.16.1.16 staðalsins ISO 27001. En eðli máls samkvæmt getur slík rannsókn ekki falið í sér kerfisbundna fyrirfram skilgreinda aðferð skv. 8. gr. reglna nr. 1221/2007 og 9. gr. reglna nr. 1222/2007 þar sem hér er um að ræða viðbrögð við atvikum sem ekki verða séð fyrir. Einnig er slík aðferð ekki í samræmi við skilgreindra aðferð Símans sjálfs um kerfisbundna framkvæmd á innra eftirliti, sbr. skjalið „[…][339]“. En þar er slíkri aðferð við framkvæmd innra eftirlits hvergi getið. Slík niðurstaða er einnig í samræmi við skýra aðgreiningu milli rannsóknar upplýsingaöryggisatvika skv. lið A.16.1.16, sbr. grein 6.1.3, og innri úttektar skv. grein 9.2 í staðlinum ISO 27001.

[338] Heiti skjals ekki birt opinberlega.
[339] Heiti skjals ekki birt opinberlega.

(166) Af öllu framangreindu leiðir því að framkvæmd Símans á innra eftirliti, m.a. til að tryggja virkni neyðaráætlunar, fyrir 12. október 2021 var ekki í samræmi við kröfur 8. gr. reglna nr. 1221/2007 og 9. gr. reglna nr. 1222/2007 þar sem það var ekki framkvæmt kerfisbundið samkvæmt fyrirfram skilgreindri aðferð.

V. Niðurstaða Fjarskiptastofu

5.1 Almennt

(167) Með bréfi, dags. 2. janúar 2024, boðaði Fjarskiptastofa fyrirhugaða ákvörðun sína vegna umrædds öryggisatviks, en þar voru forsendur og fyrirhuguð niðurstaða stofnunarinnar reifuð. Með bréfi, dags. 18. janúar 2024, barst Fjarskiptastofu athugasemdir frá Símanum vegna boðaðrar ákvörðunar stofnunarinnar.

5.2 Ný gögn og upplýsingar

(168) Í athugasemdum Símans komu fram bæði ný gögn og nýjar upplýsingar. Í bréfi Símans kom fram að fyrir mistök hafði félagið ekki sent Fjarskiptastofu allt skjáskotið af breytingarbeiðni þeirri er lá til grundvallar þeim breytingum sem verið var að vinna að þegar öryggisatvikið átti sér stað. En í því skjáskoti sem stofnunin hafði undir höndum (mynd 4) vantaði bæði stutta lýsingu á breytingunni og dagsetningar og var skjáskot sent með bréfi Símans sem innihélt þau atriði sem áður sást ekki. Fjarskiptastofa lítur þetta alvarlegum augum, sérstaklega þar sem stofnunin hafði sérstaklega spurt um þessa breytingarbeiðni ásamt öllum upplýsingum er varða hana í bréfi sínu, dags. 10. ágúst 2023.

(169) Í athugasemdum Símans kom einnig fram að þegar öryggisatvikið átti sér stað hafi verið til staðar efnislega sambærilegir viðaukar við þjónustusamning Símans við [birgi og þjónustuveitanda Símans][340] og þeir viðaukar sem Síminn hafði afhent stofnuninni sem dagsettir höfðu verið eftir að öryggisatvikið átti sér stað. Þessir viðaukar voru hins vegar ekki afhentir þegar Fjarskiptastofa fór sérstaklega fram á að þjónustusamningur Símans við [birgi og þjónustuveitanda Símans][341] yrði afhentur stofnuninni í bréfi sínu, dags. 10. ágúst 2023, og lítur stofnunin það alvarlegum augum að þeir skulu ekki hafa verið afhentir ásamt öðrum viðaukum við hann.

(170) Að lokum fylgdi með skjáskot af verklagsreglum Símans „[…][342]“ í athugasemdum félagsins. Fjarskiptastofa gerir alvarlegar athugasemdir við það að þessar verklagsreglur hafi ekki verið afhentar þegar stofnunin kallaði eftir neyðaráætlun Símans með bréfi, dags. 6. maí 2022 og þegar stofnunin óskaði sérstaklega eftir afriti af verkferlum félagsins, sem í gildi var þann 12. október 2021, fyrir gangsetningu áfallalausna með bréfi, dags. 10. ágúst 2023.

(171) Þess skal getið að þessi nýju gögn og upplýsingar breyta ekki meginforsendum ákvörðunar Fjarskiptastofu þó framangreind atriði verða vissulega leiðrétt og tekið tilliti til þeirra í ákvörðuninni á viðeigandi stöðum.

---

[340] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[341] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[342] Heiti skjals ekki birt opinberlega.

5.3 Gildissvið reglna nr. 1221/2007 og hugtakið „öryggisatvik“

(172) Í athugasemdum Símans kemur fram sú afstaða félagsins að reglur nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum eigi ekki við um atvik máls. Nánar tiltekið mótmælir Síminn að öryggi upplýsinga hafi verið ógnaði í þessu atviki. Svo kemur fram í athugasemdum Símans sú afstaða félagsins að umrætt atvik sem orsakaði útfallið hafi ekki verið „öryggisatvik“ í skilningi laga. Fjarskiptastofa telur tilefni til að bregðast við þessum athugasemdum og verður fjallaðu um þær hér að neðan.

(173) Hugtakið „upplýsingaöryggi“ er grundvallarhugtak þegar kemur að stjórnskipulagi upplýsingaöryggis. Stjórnskipulag upplýsingaöryggis er ætlað að tryggja með sem bestum hætti leynd, réttleika og tiltækileika upplýsinga og er ætlað að ná til allra upplýsinga við veitingu þjónustu, þ.m.t. upplýsinga sem þarf til að tryggja rekstur þjónustunnar, þ. á m. hönnun, þróun, rekstur, prófun og viðhald hvers kerfis, sbr. orðalag 3. tl. 7. gr. reglna nr. 1221/2007. Það er óumdeilt að stjórnskipulag upplýsingaöryggis er ætlað að tryggja virkni þjónustu aðila. Endurspeglast framangreint í skilgreiningu á „net- og upplýsingaöryggi“ í 3. gr. reglna nr. 1221/2007, þar sem hugtakið er skilgreint sem *„[h]æfni 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.*[343] *Það getur auk þess falið í sér aðra eiginleika, svo sem ósvikni, ábyrgni, óhrekjanleika og áreiðanleika.“.*

(174) Þá felst svo í hugtakinu „tiltækileiki“ að upplýsingar séu aðgengilegar og þjónusta tiltæk þegar á þarf að halda, sbr. 3. gr. reglna nr. 1221/2007.

(175) Framangreint endurspeglast einnig í alþjóðlegum viðmiðum um bestu framkvæmd á sviði upplýsingaöryggis enda byggði 47. gr. þágildandi fjarskiptalaga og reglur stofnunarinnar nr. 1221/2007 og 1222/2007 á slíkum viðmiðum. Þá er sömu nálgun að finna í gildandi lögum hér á landi um net- og upplýsingaöryggi, sbr. í 29. tl. 6. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

(176) Af framangreindum ástæðum er það mat Fjarskiptastofu að umrætt rof sem varð á þjónustu Símans hafi varðað upplýsingaöryggi, þar sem tiltækileiki upplýsinga í viðkomandi fjarskiptaneti féll niður og varð fyrir truflunum sem hafði áhrif á virkni kerfisins. Þar af leiðandi gildi ákvæði reglna nr. 1221/2007 um umrætt atvik enda gilda þær um net- og upplýsingaöryggi í fjarskiptanetum, sbr. 1. mgr. 2. gr. Auk þess sem í 1. gr. reglnanna segir að með þeim sé *„[...]kveðið á um þær ráðstafanir sem [Fjarskiptastofa] telur nauðsynlegt að fjarskiptafyrirtækin geri til að tryggja vernd umferðar og upplýsinga í almennum fjarskiptanetum. Samkvæmt þeim skal leitast við að tryggja leynd upplýsinga, lögmætan aðgang að þeim, tiltækileika þeirra og réttleika*[344]*.“.*

(177) Samkvæmt 49. tl. 3. gr. þágildandi fjarskiptalaga nr. 81/2003 telst „öryggisatvik“ vera atvik sem er gefið til kynna með einum eða fleiri óæskilegum eða óvæntum öryggisatburðum

[343] Undirstrikun Fjarskiptastofu.
[344] Undirstrikun Fjarskiptastofu.

sem talsverðar líkur eru á að stofni rekstrarþáttum í hættu og ógni upplýsingaöryggi og atvik í skilningi laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða. Skv. 48. tl. 3. gr. þágildandi fjarskiptalaga telst svo öryggisatburður vera það að upp kemur staða kerfis, þjónustu eða nets sem gefur til kynna hugsanlegt brot gegn öryggisstefnu eða bilun í öryggisráðstöfun, eða þá áður óþekkt staða sem getur skipt máli fyrir öryggi. Efnislega sama skilgreining á hugtakinu „öryggisatvik" er einnig að finna í 3. gr. reglna nr. 1222/2007 og 3. gr. reglna nr. 1221/2007. Samkvæmt framangreindu er því um öryggisatvik að ræða ef talsverðar líkur eru á því að þeir öryggisatburðir sem það veldur stofni rekstrarþáttum í hættu og ógni upplýsingaöryggi og ef um er að ræða atvik í skilningi laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða.

(178) Hugtakið „atvik" í lögum nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða er svo skilgreint sem hver sá atburður sem hefur skaðleg áhrif á öryggi net- og upplýsingakerfa, sbr. 1. tl. 6. gr. þeirra laga.

(179) Afleiðingar umrætts atviks fólust í því að þann 12. október 2021 frá kl. 11:30 - 12:02 varð rof á farsíma- og farnetsþjónustu Símans og á hluta fastlínukerfa Símans. Er óumdeilt að fjarskiptaþjónusta, sem sannarlega er einn veigamesti rekstrarþáttur félagsins, féll niður að hluta vegna atviksins og er það því mat Fjarskiptastofu að rekstrarþáttum hafi eðli máls samkvæmt verið stofnað í hættu, eða a.m.k. talsverðar líkur hafi verið á því. Einnig er það mat Fjarskiptastofu að umrætt rof sem varð á þjónustu Símans hafi varðað upplýsingaöryggi, þar sem tiltækileiki upplýsinga í viðkomandi fjarskiptaneti féll niður sem hafði áhrif á virkni kerfisins. Þar af leiðandi hafi umrætt atvik verið „öryggisatvik" í skilningi framangreindra réttarheimilda. Af framangreindum ástæðum er því andmælum Símans hafnað.

<u>5.4 Staðlar</u>

(180) Í athugasemdum Símans virðist koma fram að félagið telji að ISO-27001 staðallinn, sem vísað var til í boðaðri ákvörðun, hafi verið notaður sem réttarheimild og er því mótmælt. Einnig kemur þar fram, og því jafnframt mótmælt, að fjarskiptafélögum sé skylt að vera vottuð skv. staðlinum. Fjarskiptastofa telur tilefni til að bregðast við þessum athugasemdum og verður fjallaðu um þær hér að neðan.

(181) Samkvæmt þágildandi fjarskiptalögum nr. 81/2003 kemur fram í 2. og 3. mgr. 47. gr. laganna að Fjarskiptastofa setji reglur um vernd upplýsinga í almennum fjarskiptanetum þar sem nánar er mælt fyrir um þær kröfur sem gerðar eru til skipulags upplýsingaöryggis og að stofnunin setji sérstakar reglur um virkni almennra fjarskiptaneta. Svo segir þar að reglurnar skuli m.a. kveða á um hlítingu við tiltekna staðla, sbr. b. lið 1. og 2. mgr. 47. gr.

(182) Á grundvelli framangreinds ákvæðis þágildandi fjarskiptalaga hefur Fjarskiptastofa sett bæði reglur nr. 1221/2007 og reglur nr. 1222/2007. En bæði reglurnar og 47. gr. þágildandi fjarskiptalaga byggja á alþjóðlegum viðmiðum um bestu framkvæmd á sviði upplýsingaöryggis. Svo er kveðið á um það í 3. mgr. 2. gr. reglna nr. 1221/2007 og 4. gr. reglna nr. 1222/2007 að:

> *Til hliðsjónar má styðjast við staðlana ISO/IEC 27001 (Stjórnkerfi upplýsingaöryggis) og ISO/IEC 17799 (Starfsvenjur fyrir stjórnun upplýsingaöryggis). Fara skal eftir nýjustu útgáfu*

staðlanna á hverjum tíma. Staðlana má ennfremur nota sem leiðbeiningar um ráðstafanir sem innleiða má til að uppfylla kröfur reglnanna.

(183) Af öllu framangreindu er því ljóst að, af svo miklu leyti sem ákvæði reglnanna gangi ekki lengra en ákvæði staðlana, ber að skýra ákvæði reglnanna til samræmis við þá enda gera reglurnar ráð fyrir að hægt sé að nota þá við hlítni við þær. Umræddir staðlar eru því hvorki notaðir í ákvörðun þessari sem réttarheimild né heldur er gerð krafa til fjarskiptafélaga að þau hafi vottun skv. þeim. Til þess ber þó að líta að Síminn hefur verið með ISO/IEC vottun fyrir stjórnkerfi upplýsingaöryggis síðan 12. maí 2016 og hefur því notað þá staðla við hlítni við ákvæði umræddra reglna.

5.5 Varabúnaður

(184) Í athugasemdum Símans kemur fram að félagið telji að ekki sé gætt samræmis í ákvörðunum Fjarskiptastofu í sambærilegum málum hvað varðar kröfur til varabúnaðar, og er þar vísað til nýlegrar ákvörðunar stofnunarinnar nr. 6/2023. Fjarskiptastofa hafnar þessum andmælum þar sem ekki var um sambærileg atvik að ræða. Í því máli sem Síminn bendir á var um að ræða litla breytingu á fjarskiptaneti sem tók stuttan tíma, en í því máli sem um ræðir í ákvörðun þessari var um að ræða verulegar breytingu sem tók langan tíma, og er því ekki um sambærileg atvik að ræða.

(185) Þegar áætlað er að uppfæra farsímakjarna fjarskiptafélags sem standa á yfir í meira en 14 vikur, þar […][345], verður að gera þá kröfur að til staðar sé nægur varabúnaður og önnur úrræði til að viðhalda samfelldum rekstri meðan á uppfærslunni stendur í samræmi við kröfur 4. mgr. 20. gr. reglna nr. 1222/2007.

5.6 Útvistun

(186) Í athugasemdum Símans kemur fram að félagið telur að sú þjónusta sem Síminn kaupir af [birgi og þjónustuveitanda Símans][346] skv. umræddum þjónustusamningi teljist ekki til útvistunar. Í athugasemdunum kemur fram að *„Það eitt að kaupa þjónustu frá ytri aðila sem tengist að einhverju leyti rekstri félagsins á búnaði eða kerfi, felur ekki þá þegar í sér að rekstur kerfisins sé útvistaður.“.* Svo segir í athugsemdum Símans:

> [...]*hefur Síminn alltaf haft þann skilning að útvistun á rekstri feli í sér mun umfangsmeiri aðgerð en að gera þjónustusamning. Útvistun á kerfi hlýtur að fela í sér að ákvörðunarvald yfir veigamiklum atriðum tengd rekstrinum er fært yfir til þriðja aðila.*

(187) Svo segir einnig í athugasemdunum:

> *Að mati Símans felur útvistun í sér mun umfangsmeira hlutverk til handa þjónustuveitanda og felur sérstaklega í sér ákvörðunartöku um hvernig málum skuli háttað í rekstrinum[...]*

(188) Fjarskiptastofa telur tilefni til að bregðast við þessum athugasemdum og verður fjallað um þær hér að neðan.

---

[345] Hluti ákvörðunar ekki birt opinberlega.
[346] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

(189) Ákvæði 1. máls. 1. mgr. 13. gr. reglna nr. 1221/2007 kveður á um að fjarskiptafyrirtæki sé heimilt að semja við þriðja aðila um að annast, í heild eða að hluta, rekstur fjarskiptanets. Síminn hefur haldið því fram að útvistun á fjarskiptakerfi hljóti að fela í sér að ákvörðunarvald yfir veigamiklum atriðum tengdum rekstrinum sé fært yfir til þriðja aðila og þar með hafi Síminn ekki útvistað rekstri til [birgis og þjónustuveitanda Símans][347] með því að fela félaginu þá starfsemi sem þjónustusamningurinn kveður á um. Það verður hins vegar ekki séð hvaða ákvörðunarvald yfir veigamiklu atriðum Síminn er að vísa til þar sem 2. máls. 1. mgr. 13. gr. reglnanna kveður á um að stjórnunarlegri ábyrgð og áhættustýringu verði ekki útvistað og þar með að slíkt sé ekki heimilt.

(190) Af framangreindu leiðir því að það er ekki hægt að túlka orðið „rekstur" í 13. gr. reglnanna með jafn þröngum hætti og Síminn heldur fram. Slíkt er einnig í samræmi við notkun orðsins í öðrum ákvæðum reglnanna og þágildandi fjarskiptalaga, en þar er orðið „rekstur" notað með rúmum hætti um hverskonar rekstur eða starfsemi fjarskiptafélags, t.d. *áætlun um samfelldan rekstur* í 9. gr. reglna nr. 1221/2007. Það að annast rekstur fjarskiptanets að hluta fyrir hönd útvistunaraðila felur því í sér að annast ákveðinn rekstur eða starfsemi er varðar fjarskiptanet undir stjórnunarlegri ábyrgð og áhættustýringu þess aðila sem útvistar.

(191) Þess skal einnig getið að skv. 1. máls. 1. mgr. 13. gr. reglnanna er ekki kveðið á um neinn neðri þröskuld hvað varðar orðið „að hluta" í því ákvæði og þarf því útivistun ekki að vera umfangsmikil til að falla undir ákvæðið og teljast til útvistunar að hluta.

(192) Samkvæmt þjónustusamningi Símans við [birgi og þjónustuveitanda Símans][348] þá annast sá síðarnefndi kerfisbundna aðstoð og ráðgjöf auk þess að framkvæma vinnu við uppfærslur og uppsetningar í tengslum við fjarskiptanet félagsins er varðar virkni fjarskiptanets félagsins, en slík starfsemi er óhjákvæmilega hluti af rekstri fjarskiptanets. Með því að fela [birgi og þjónustuveitanda Símans] þennan rekstur með þjónustusamningi er því Síminn ekki að sinna þessum rekstri heldur hefur félagið útvistað þessum rekstri fjarskiptanetsins til [birgis og þjónustuveitanda Símans]. Í þessu samhengi er vakinn athygli á því að [birgir og þjónustuveitandi Símans][349] hafði […][350] sem voru andlag umrædds þjónustusamnings og að […][351] að umræddum fjarskiptanetum Símans. Af því leiðir að skv. framangreindum þjónustusamningi hefur [birgi og þjónustuveitanda Símans][352] verið falið að annast framangreinda starfsemi varðandi rekstur fjarskiptanets Símans og þar með rekstur fjarskiptanets Símans að hluta í skilningi 1. og 2. málsl. 1. mgr. 13. gr. reglna nr. 1221/2007. Af framangreindum ástæðum er því andmælum Símans hafnað.

5.7 Aðgangsstýring

(193) Í athugasemdum Símans kemur eftirfarandi fram:

---

[347] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[348] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[349] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[350] Hluti ákvörðunar ekki birt opinberlega.
[351] Hluti ákvörðunar ekki birt opinberlega.
[352] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.

Þá telur FST að Síminn hafi brotið gegn 6. tölul. 12. gr. reglna nr. 1221/2007 þar sem sá starfsmaður [birgis og þjónustuveitanda Símans][353] sem olli atvikinu hafði verið […][354] að fjarskiptakerfi Símans án þess að þurfa þess, að mati FST, í ljósi þess sem sagði í frávikaskýrslu [birgis og þjónustuveitanda Símans][355]. Í þessu samhengi skal bent á að það eina sem hefði mögulega komið í veg fyrir áhrif þessara mannlegu mistaka með öllu hefði verið annars konar aðgangsheimild[356].

(194) Samkvæmt þessu er því Síminn sammála því mati Fjarskiptastofu að það að takmarka betur aðgangsheimildir viðkomandi starfsmanns við framkvæmd umrædds starfs hefði komið í veg fyrir öryggisatvikið með öllu. Hins vegar segir síðan eftirfarandi í athugasemdunum:

[…][357]

(195) Af þessu mætti ætla að starfsmanninum hafi því ekki verið unnt að framkvæma það verk sem honum var ætlað að sinna þegar atvik máls áttu sér stað með […][358]. Hins vegar er síðar í athugasemdunum dregið í land með það og sagt að það sé einungis erfitt að takmarka aðgangsheimildir, en þar segir:

Varðandi þetta atriði, um mögulegar breytingar á högun aðgangsstýringar, var niðurstaðan sú að það væru afar erfitt að gera miklar breytingar á því[359] […][360] fyrir starfsfólk [birgis og þjónustuveitanda Símans][361] sem kemur að þjónustu til Símans.

(196) Samkvæmt athugasemdum Símans er því „afar erfitt" að framkvæma þær breytingar á aðgangsstýringu sem frávikaskýrsla [birgis og þjónustuveitanda Símans][362] kveður á um að nauðsynlegar séu til að koma í veg fyrir svipuð atvik í framtíðinni. Þess skal getið að í frávikaskýrslu [birgis og þjónustuveitanda Símans][363] er afdráttarlaust kveðið á um að einungis […][364] þá vinnu sem framkvæmd var. Í frávikaskýrslunni segir um það hvernig til tókst með framkvæmd þeirra úrbóta sem [birgir og þjónustuveitandi Símans][365] lagði til, að það sé ekki auðvelt, hins vegar kemur hvergi fram að það sé ekki hægt, en þar segir nánar tiltekið:
366

Not easy to fully implement, but the partie are now more stricly and higher focus on the […][367].

[353] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[354] Hluti bréfs ekki birtur opinberlega.
[355] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[356] Undirstrikun Fjarskiptastofu.
[357] Hluti bréfs ekki birt opinberlega.
[358] Hluti ákvörðunar ekki birt opinberlega.
[359] Undirstrikun Fjarskiptastofu.
[360] Hluti bréfs ekki birt opinberlega.
[361] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[362] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[363] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[364] Hluti ákvörðunar ekki birt opinberlega.
[365] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[366] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[367] Hluti bréfs ekki birt opinberlega.

(197) Af frávikaskýrslu [birgis og þjónustuveitanda Símans][368] og ummælum í athugasemdum Símans er því ljóst að erfitt var að framkvæma þær breytingar sem um ræðir en ekki ómögulegt. Jafnvel þó Síminn segi það á einum stað í athugasemdum sínum að það sé ekki hægt, er það svo jafnskjótt dregið til baka og sagt að það sé einungis „afar erfitt“. Einnig skal það tekið fram að þær úrbætur á aðgangsstýringu sem kveðið er á um í frávikaskýrslu [birgis og þjónustuveitanda Símans][369] varðar einungis umrætt tilvik, þ.e. þá vinnu við vandræðaveiðar í kjölfar uppfærslunnar í […][370], þær gilda því ekki endilega um annan aðgang starfsmanna [birgis og þjónustuveitanda Símans][371] í kerfi Símans sem varðar t.d. bilanagreiningu eða önnur viðbrögðum við bilunum.

(198) Þar sem frávikaskýrsla [birgis og þjónustuveitanda Símans][372] er afdráttarlaus um það að félagið telji að aðgangsheimild umrædds starfmanns þess hafi verið […][373] og að það hafi verið ein orsök umrædds öryggisatviks, og með vísan til þess að þegar öryggisatvikið gerðist var um að ræða mjög áhættusaman hluta uppfærslunnar þar sem tenging var kominn milli farsímakjarnanna, þá er ljóst að ekki var með fullnægjandi hætti takmarkaður aðgangur umrædds starfsmanns [birgis og þjónustuveitanda Símans][374] að upplýsingum við þær sem honum var nauðsynlegt til að hann gæti sinnt starfi sínu, þar sem hann hafði […][375]. Skiptir í þessu samhengi ekki máli hvort erfitt hafi verið að framkvæma þær breytingar á aðgangsstýringu sem um ræðir enda er hér um meginorsök öryggisatviksins að ræða. Af framangreindum ástæðum er því andmælum Símans hafnað.

5.8 Niðurstöður

(199) Hér að framan hefur verið gerð grein fyrir þeim álitamálum sem Fjarskiptastofa telur að hafi komið upp vegna öryggisatviks sem átti sér stað í fjarskiptaneti Símans þann 12. október 2021.

(200) Að mati Fjarskiptastofu leiðir stjórnsýsluskoðun stofnunarinnar í ljós töluverða annmarka í öryggisskipulagi Símans að því er snertir öryggisatvik þessa máls. Hins vegar ber að líta til þess að þegar upp komst um útfallið var brugðist hratt við enda tók endurreisn skamman tíma.

(201) Lýsa þessir annmarkar sér í því að áætlað var að vinna að uppfærslum í kjarnakerfi félagsins yfir 14 vikna tímabil án þess að viðhaft sé verklag sem samræmist að öllu leyti kröfum um stjórnskipulag upplýsingaöryggis.

(202) Það er mat Fjarskiptastofu að Síminn hafi metið áhrif og líkur vegna umræddra breytinga en að áhættustig hafi ekki verið reiknað út og borið saman við fyrirframgerðan mælikvarða um

[368] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[369] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[370] Hluti ákvörðunar ekki birt opinberlega.
[371] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[372] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[373] Hluti ákvörðunar ekki birt opinberlega.
[374] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[375] Hluti ákvörðunar ekki birt opinberlega.

ásættanlegt áhættustig um öryggi upplýsinga, órofinn rekstur og þjónustustig. Því hafi sú hætta sem steðjaði að fjarskiptaneti Símans ekki verið áhættumetin með fullnægjandi hætti þegar umrætt öryggisatvik átti sér stað. En slíkt er ekki í samræmi við kröfur 7. gr. reglna nr. 1222/2007, sbr. 2. tl. 7. gr. reglna nr. 1221/2007.

(203) Það er svo mat Fjarskiptastofu að Síminn hafi útvistað rekstri fjarskiptaneta sinna að hluta til [birgis og þjónustuveitanda Símans][376] með þjónustusamningi, en það félag framkvæmdi umræddar breytingar sem olli öryggisatvikinu. Hins vegar var ekki rétt staðið að útvistuninni og var þjónustusamningur Símans við [birgi og þjónustuveitanda Símans][377] ekki í samræmi við kröfur 13. gr. reglna nr. 1221/2007 þar sem ekki var þar kveðið á um skyldu [birgis og þjónustuveitanda Símans][378] til að starfa í samræmi við fyrirmæli Símans og ákvæði reglna nr. 1221/2007, ekki var kveðið á um ákvæði um þagnarskyldu og þar með tryggt að farið sé að ákvæðum fjarskiptalaga þar að lútandi og ekki var kveðið á um ákvæði sem tryggðu Fjarskiptastofu aðgang að upplýsingum frá [birgi og þjónustuveitanda Símans][379] og að stofnunin gæti í þágu eftirlits framkvæmt athuganir á starfsstöð félagsins.

(204) Umrædd breyting var samþykkt í heild sinni á fundi breytingaráðs Símans þann 26. ágúst 2021, þ.e. tæpum tveimur mánuðum áður en að breyting var framkvæmd. Hins vegar var breytingarbeiðnin sem samþykkt var og lá til grundvallar breytingunum takmörkuð og óljós. Einnig er það mat stofnunarinnar að þær verklagsreglur sem unnið var eftir við gerð breytingarbeiðninnar hafi verið ófullnægjandi þar sem þær kváðu ekki á um með skýrum hætti hvaða efnisatriði breytingabeiðnir félagsins skuli innihalda eða hvernig meta eigi hvaða efnisatriði þær skuli innihalda. Verklagsreglurnar kváðu heldur ekki á um þá venju Símans að framkvæma skyldi allar breytingar sem gætu haft áhrif á notendur að nóttu til a.m.k. þegar stendur til að „slökkva“ á virkum, lifandi kerfum sem gæti haft áhrif á þjónustu til viðskiptavina félagsins. Af framangreindu leiðir því að verkferlar Símans sem fjölluðu um breytingar tryggðu ekki viðeigandi formlega meðhöndlun breytinga ásamt skjalfestingu þeirra og höfðu ekki í för með sér traustan, skipulegan og fyrirsjáanlegan rekstur fjarskiptaneta en slíkt er ekki í samræmi við kröfur 1. mgr. 23. gr. reglna nr. 1222/2007.

(205) Það er einnig mat Fjarskiptastofu að aðgangur þess starfsmanns [birgis og þjónustuveitanda Símans][380] sem var að vinna að þeim breytingum sem olli umræddu öryggisatviki hafi ekki verið takmarkaður við þær upplýsingar sem honum var nauðsynlegt til að hann gæti sinnt starfi sínu, þar sem [...][381]. En slíkt er ekki í samræmi við kröfur 6. tl. 12. gr. reglna nr. 1221/2007.

(206) Breytingin sem framkvæmd var á fjarskiptaneti Símans í […][382] um kl. 11:30 þann 12. október 2021 var svo ekki framkvæmd þannig að hún truflaði sem minnst fjarskiptaþjónustu Símans þar sem félagið fór ekki eftir sínum eigin verklagsreglum við framkvæmd umræddra

[376] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[377] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[378] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[379] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[380] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[381] Hluti ákvörðunar ekki birt opinberlega.
[382] Hluti ákvörðunar ekki birt opinberlega.

breytinga, þar sem félagið […][383], og engar prófanir fóru fram áður en breytingarnar voru framkvæmdar. En slíkt er ekki í samræmi við kröfur 2. mgr. 23. gr. reglna nr. 1222/2007.

(207) Það er því mat Fjarskiptastofu að Síminn hafi hvorki haft þá yfirsýn yfir breytingarnar né stjórn á þeim líkt og ákvæði laga og afleiddra reglna gera kröfu um. En eins og fram kemur í ákvörðun þessari má rekja orsök öryggisatviksins til þess að sá starfsmaður […][384] og félagið hafi ekki stjórnað þeim aðgangi með fullnægjandi hætti. En öryggisatvikið varð til þess að útfall varð á þjónustu til allt að 150.000 notenda Símans í yfir 30 mínútur þann 12. október 2021, þ.e. frá kl. 11:30 - 12:02.

(208) Það er einnig mat Fjarskiptastofu að ekki hafi verið til staðar nægur varabúnaður og önnur úrræði þegar öryggisatvikið átti sér stað til að viðhalda samfelldum rekstri en slíkt er ekki í samræmi við kröfur 4. mgr. 20. gr. reglna nr. 1222/2007.

(209) Það er svo niðurstaða stofnunarinnar að neyðaráætlun Símans hafi verið ófullnægjandi þar sem ekki kom fram í henni lýsing á viðhaldi handbóka fyrir daglegan rekstur búnaðar og ekki komu þar fram skilgreining á hámarkstíma rekstrarstöðvunar áður en gripið er til áætlunarinnar en slíkt er ekki í samræmi við þær kröfur sem leiða af. 2. og 4. tl. 8. gr. reglna nr. 1222/2007. Einnig er það mat Fjarskiptastofu að neyðaráætlunin hafi ekki verið prófuð reglulega til að tryggja virkni hennar áður en umrætt öryggisatvik átti sér stað en slíkt er ekki í samræmi við kröfur 8. gr. reglna nr. 1222/2007. Að lokum er það svo mat Fjarskiptastofu að ekki hafi verið til staðar fullnægjandi innra eftirlit, m.a. til að tryggja virkni neyðaráætlunar, þar sem það var ekki framkvæmt kerfisbundið samkvæmt fyrir fram skilgreindri aðferð, en slíkt er ekki í samræmi við kröfur 9. gr. reglna nr. 1222/2007 og 8. gr. reglna nr. 1221/2007.

Á k v ö r ð u n a r o r ð

1. **Áhættumat þeirra breytinga sem framkvæmdar voru á fjarskiptaneti Símans í […][385] um kl. 11:30 þann 12. október 2021 var ófullnægjandi þar sem áhættustig var ekki reiknað út og borið saman við fyrirframgerða mælikvarða um ásættanlegt áhættustig um öryggi upplýsinga, órofin rekstur og þjónustustig en slíkt er ekki í samræmi við kröfur 1. mgr. 7. gr. reglna nr. 1222/2007, sbr. 5. málsl. 2. tl. 7. gr. reglna nr. 1221/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.**

2. **Þegar breytingar voru framkvæmdar á fjarskiptaneti Símans í […][386] um kl. 11:30 þann 12. október 2021 var þjónustusamningur Símans við [birgi og þjónustuveitanda**

[383] Hluti ákvörðunar ekki birt opinberlega.
[384] Hluti ákvörðunar ekki birt opinberlega.
[385] Hluti ákvörðunar ekki birt opinberlega.
[386] Hluti ákvörðunar ekki birt opinberlega.

Símans][387] ekki í samræmi við þær kröfur sem leiða af 1., 3. og 5. tl. 13. gr. reglna nr. 1221/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.

3. **Þegar framkvæmdar voru breytingar á fjarskiptaneti félagsins í […][388] um kl. 11:30 þann 12. október 2021 tryggðu verkferlar Símans sem fjölluðu um breytingar ekki viðeigandi formlega meðhöndlun breytinga ásamt skjalfestingu þeirra og höfðu ekki í för með sér traustan, skipulegan og fyrirsjáanlegan rekstur fjarskiptaneta en slíkt er ekki í samræmi við kröfur 1. mgr. 23. gr. reglna nr. 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.**

4. **Þegar breytingar voru framkvæmdar á fjarskiptaneti Símans í […][389] um kl. 11:30 þann 12. október 2021 þá hafði aðgangur þess starfsmanns sem var að vinna að þeim ekki verið takmarkaður við þær upplýsingar sem honum var nauðsynlegt til að hann gæti sinnt starfi sínu en slíkt er ekki í samræmi við kröfur 6. tl. 12. gr. reglna nr. 1221/2007.**

5. **Sú breyting sem framkvæmd var á fjarskiptaneti Símans í […][390] um kl. 11:30 þann 12. október 2021 var ekki framkvæmd þannig að hún truflaði sem minnst fjarskiptaþjónustu félagsins en slíkt er ekki í samræmi við kröfur 2. mgr. 23. gr. reglna nr. 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.**

6. **Þegar breytingar voru framkvæmdar á fjarskiptaneti Símans í […][391] um kl. 11:30 þann 12. október 2021 var ekki til staðar nægur varabúnaður og önnur úrræði til að viðhalda samfelldum rekstri en slíkt er ekki í samræmi við kröfur 4. mgr. 20. gr. reglna nr. 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.**

7. **Þegar öryggisatvikið átti sér stað 12. október 2021 var neyðaráætlun Símans ekki í samræmi við þær kröfur sem leiða af. 2. og 4. tl. 8. gr. reglna nr. 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.**

8. **Þegar öryggisatvikið átti sér stað 12. október 2021 hafði neyðaráætlun Símans ekki verið prófuð reglulega til að tryggja virkni hennar en slíkt er ekki í samræmi við kröfur 8. gr. reglna nr. 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.**

9. **Þegar öryggisatvikið átti sér stað 12. október 2021 var ekki til staðar fullnægjandi innra eftirlit til að tryggja virkni neyðaráætlunar þar sem það var ekki framkvæmt kerfisbundið samkvæmt fyrirfram skilgreindri aðferð en slíkt er ekki í samræmi við kröfur 9. gr. reglna nr. 1222/2007 og 8. gr. reglna nr. 1221/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.**

[387] Nafn birgis og þjónustuveitanda Símans ekki birt opinberlega.
[388] Hluti ákvörðunar ekki birt opinberlega.
[389] Hluti ákvörðunar ekki birt opinberlega.
[390] Hluti ákvörðunar ekki birt opinberlega.
[391] Hluti ákvörðunar ekki birt opinberlega.

Fjarskiptastofa, 20. mars 2024

____

Hrafnkell V. Gíslason

____

Björn Þór Rögnvaldsson