Ákvörðun nr. 6/2023
Öryggisatvik hjá Sýn hf.

(mál nr. 2022080003)

I.
Almennt

(1) Þann 13. júlí 2022 kom upp öryggisatvik hjá Sýn hf. (hér eftir Sýn) sem varð til þess að tveir öryggisatburðir áttu sér stað. Barst Fjarskiptastofu atvikaskýrsla vegna öryggisatviksins 14. júlí 2022 eftir að stofnunin hafði óskaði eftir upplýsingum um atvikið., sbr. skjalið *„REK-26245-Atvikaskýrsla vegna útfalls á símkerfi Vodafone.pdf.“ (hér eftir nefnt atvikaskýrsla)*.

(2) Fjarskiptastofa hóf forskoðun á öryggisatvikinu með bréfi, dags. 2. ágúst 2022, og óskaði frekari upplýsinga frá félaginu með bréfi, dags. 15. september 2022. Eftir yfirferð á gögnum frá félaginu var það niðurstaða forskoðunar að hefja stjórnsýsluskoðun á umræddum öryggisatviki. Var félaginu tilkynnt um þá niðurstöðu með bréfi, dags. 13. október 2022, ásamt því að frekari upplýsinga var aflað.

II.
Forskoðun öryggisatviks hjá Sýn

2.1 Öryggisatvikið

(3) Þann 13. júlí 2022 varð öryggisatvik hjá Sýn sem olli alvarlegu rofi og truflunum á fastlínuþjónustu og farsímaþjónustu fyrirtækisins. Strax hafði rofið veruleg áhrif á farsímanotendur og var fjallað um það í fréttum fjölmiðla[1]. Í niðurstöðukafla áðurnefndrar atvikaskýrslu Sýnar segir:

[1] https://www.ruv.is/frett/2022/07/13/bilun-i-simkerfi-hja-vodafone?term=bilun%20%C3%AD%20s%C3%ADmkerfi%20hj%C3%A1%20vodafone&rtype=news&slot=1

- Breytingar sem voru gerðar í báðum kjarnaeiningum fastlínukerfa Vodafone kl. 06:10 höfðu óvæntar afleiðingar í för með sér en samskonar breytingar hafa verið gerðar nokkum sinnum áður án þess að upp hafi komið vandamál.
- Breytingarstjórnunarferli var ekki fylgt með réttum hætti sem hafði veruleg áhrif á því hvernig að atvikið átti sér stað og hvaða áhrif málið hafði á þjónustu viðskiptavina.
- Atvikið olli rofi á Fastlínusímaþjónustu Vodafone og símtölum milli farsímakerfis Vodafone og annara fjarskiptafyrirtækja á milli kl. 06:10 – 07:50.
- Afmarkaðar truflanir urðu einnig milli kl. 09:15 – 10:35 sem höfðu meðal annars áhrif á OneNet og afgreiðslu símtala.
- Allar aðgerðir voru framkvæmdar meðan bilun stóð yfir og ekki þörf á frekari aðgerðum tengdu þessu atviki.

(4) Hvað varðar aðgerðir félagsins og úrbætur vegna öryggisatviksins, þá kemur eftirfarandi fram í atvikaskýrslunni:

Farið verður yfir verklag vegna breytinga og bætt úr fylgni við breytingarstjórnunar ferli Vodafone sem tekur meðal annars á:
- *Mati á áhættu vegna breytinga*
- *Dregur úr áhættu á þjónustuskerðingu vegna breytinga*
- *Eftirliti og prófunum eftir breytingar*
- *Endurheimt þjónustu ef breytingar misfarast*
- *Upplýsingagjöf og tilkynningar til hagsmunaaðila*

(5) Líkt og áður segir hóf Fjarskiptastofa forskoðun á umræddu öryggisatviki með bréfi, dags. 2. ágúst 2022. Í bréfi stofnunarinnar til félagsins var óskað ítarlegri upplýsinga er varða tildrög atviksins, 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 óskað eftirfarandi:

1. *Lýsingu á þeirri atburðarás sem átti sér stað í júlí sl. sem leiddi til þjónusturofs og/eða truflana.*
2. *Lýsingu á þeirri þjónustu sem rofnaði og/eða varð fyrir truflunum í júlí sl.*
3. *Lýsingu 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 og/eða hvort neyðaráætlun var virkjuð. Óskað er eftir afriti af neyðaráætlun og breytingarstjórnunarferli Sýn hf.*
4. *Lýsingu á þeim áhrifum sem þjónusturofið hafði á, a) kerfi félagsins, og b) viðskiptavini þess, þ.m.t. en ekki einskorðað við fjölda notenda, umfang og niðritíma þjónustunnar.*
5. *Lýsingu á þeim úrbótum sem Sýn hf. ætlar að gera til að koma í veg fyrir að svipuð atvik endurtaki sig.*

(6) Stofnuninni barst svar frá félaginu þann 16. ágúst 2022 og samanstóð það af bréfi með svörum við spurningum Fjarskiptastofu ásamt tveimur skjölum *„breytingarstjornunarferli.pdf“* og *„Neyðaráætlun Sýnar.pdf“.*

(7) Í svari Sýnar, dags. 16. ágúst 2022, kom fram að öryggisatvikið átti sér stað eftir að breytingar voru gerðar í miðlægum símkerfabúnaði félagsins. Fljótlega eftir að breytingarnar voru gerðar fékk stjórnborð Sýnar upplýsingar um óeðlilega hegðun og voru viðbrögð félagsins að virkja neyðaráætlun þess og kalla út bakvakt, auk þess að óska eftir aðstoð frá framleiðanda búnaðarins. Unnið var að greiningu og í kjölfarið voru gerðar lagfæringar á símkerfinu þannig að afgreiðsla símtala og þjónusta félagsins komst í eðlilegt horf. Umræddar lagfæringarnar reyndust þó ekki nægilegar þar sem klukkutíma síðar kom á ný í ljós óeðlileg hegðun í fastlínukerfi félagsins sem hafði þær afleiðingar að hluti símtala var ekki að virka eðlilega. Önnur greining ásamt frekari lagfæringum voru því gerðar og komst þá eðlileg þjónusta á.

(8) Hvað varðar svar Sýnar við annarri spurningu Fjarskiptastofu þá var það efnislega sambærilegt þeim upplýsingum sem fram komu í atvikaskýrslu félagsins. Í svarinu Sýnar, dags. 16. ágúst 2022, segir:

> *Atvikið olli rofi á fastlínusímaþjónustu Vodafone og símtölum milli farsímakerfis Vodafone og annara fjarskiptafyrirtækja á milli kl. 06:10 – 07:50.*
> *Afmarkaðar truflanir urðu einnig milli kl. 09:15 – 10:35 [...]*[2]

(9) Sýn greindi frá því í svari sínu við fjórðu spurningu Fjarskiptastofu að áhrif þjónusturofsins voru þau að „[f]*astlínunotendur Vodafone voru sambandslausir og einnig* [voru] *símtöl milli farsímakerfis Vodafone og annarra fjarskiptafyrirtækja úti. Hins vegar voru símtöl innan farsímakerfis Vodafone í lagi.“*.

(10) Jafnframt lýsir Sýn því í svari sínu við fimmtu spurningu Fjarskiptastofu að eftir atvikið hafi verið farið yfir breytingarstjórnunarferli félagsins með starfsfólkinu. Var brýnt fyrir starfsfólki mikilvægi áhættumats, framkvæmd prófana og eftirlit með breytingum, endurheimt þjónustu, upplýsingagjöf og tilkynningar til hagsmunaaðila.

(11) Gögn málsins sýna að Sýn hefur skjalfesta verklagsreglu um breytingarstjórnunarferlið, sbr.: skjalið „Breytingastjórnunarferli.pdf.“. Í skjalinu er tilgreint eftirfarandi markmið:

> *Markmið breytingastjórnunar er að bregðast skilvirkt við breytingum á kröfum viðskipta og IT. Breytingastjórnun tryggir staðlaðar aðferðir, bætir upplýsingamiðlun og dregur úr áhættu á skertri þjónustu til viðskiptavina vegna breytinga sem framkvæmdar eru.*

(12) Þá er þar einnig að finna skilgreiningu á því hvað telst vera breyting og til hvaða breytinga ferlið nær til. Þar segir:

> *[....]*[3]

(13) Í áðurnefndri verklagsreglu um breytingastjórnunarferli Sýnar er skilgreint verklag við breytingar. Er þar sett fram ákveðin flokkun breytinga og er verklag við breytingar sem flokkast sem almennar breytingar (e. Standard change) eftirfarandi:

[2] Efni hluta bréfsins ekki birt opinberlega.
[3] Efni hluta verklagsreglnanna ekki birt opinberlega.

1) Breytingarbeiðni skráð og þar sem um standard change er hún fyrirfram samþykkt,
2) Rekstrartruflun skráð,
3) Breyting framkvæmd,
4) Breytingu lokið ef vel heppnuð framkvæmd, en ef ekki er
5) „Rollback".

(14) Í breytingastjórnunarferli Sýnar er skilgreindur sérstakur tímarammi eða vinnugluggi þar sem heimilt er að framkvæma breytingar í kerfum félagsins. Þar segir:

[...][4]

(15) Við yfirferð Fjarskiptastofu mat stofnunin að þörf væri á að afla frekari upplýsinga um öryggisatvikið, viðbrögð Sýnar við þeim sem og stjórnskipulag félagsins áður en tekin væri ákvörðun um hvort hefja ætti stjórnsýsluskoðun.

(16) Fjarskiptastofa kallaði því eftir frekari upplýsingum með fyrirspurn í bréfi, dags. 15. september 2022. Þá var jafnframt óskað eftir að félagið myndi afhenda stofnuninni gögn sem myndu styðja við svör félagsins. Nánar tiltekið var óskað eftirfarandi:

1. *Í svari félagsins frá 16. ágúst er tilgreint að öryggisatvikið olli rofi á fastlínuþjónustu og símtölum milli farsímakerfis Vodafone og annara fjarskiptafyrirtækja [...]*[5]*. Óskað eftir nánari útskýringu á hvaða þjónustur félagsins urðu fyrir rofi.*
2. *Í svari félagsins frá 16. ágúst kemur fram að um var að ræða alvarlegt útfall sem hafði m.a. þau áhrif að fastlínunotendur Vodafone voru sambandslausir. Óskað er eftir upplýsingum um hvert var umfang útfallsins, náði það til allra fastlínunotenda eða hluta þeirra. Óskað eftir tölulegum upplýsingum um fjölda sem urðu fyrir áhrifum og til hvaða landsvæða útfallið náði.*
3. *Í svari Sýnar dags 16. ágúst sl. kemur fram að breytingarstjórnunarferli Sýnar hafi ekki verið fylgt á réttan hátt þann 13. Júlí. Óskað er lýsingu því verklagi sem var viðhaft og hvernig hafi verið vikið frá settu verklagi.*
4. *Óskað er eftir skýringu á flokkunarkerfi útfalla, þ.e. A, B og C, en til slíkrar flokkunar er vísað í breytingarstjórnunarferli sem fylgdi svarbréfi félagsins dags. 16. ágúst sl.*
5. *Óskað er eftir afriti af breytingabeiðni fyrir þá breytingu sem framkvæmd var á morgni 13. júlí og leiddi til öryggisatvikanna.*
6. *Óskað er eftir afriti af tilkynningum sem fóru til viðskiptavina þann 13. júlí sl. vegna umrædda öryggisatvika.*
7. *Óskað er eftir afriti af skjalfestri aðferðafræði áhættumats Sýnar um upplýsingaöryggi og áhættumati breytinga.*

(17) Stofnuninni barst svar frá félaginu, sbr. bréf dags. 20. september 2022. Svar félagsins samanstóð af bréfi með svörum við spurningum Fjarskiptastofu ásamt þremur öðrum

[4] Efni hluta verklagsreglnanna ekki birt opinberlega.
[5] Efni hluta bréfsins ekki birt opinberlega

skjölum, þ.e. *„Viðauki II Verklag áhættustýringar.pdf“, „Viðauki III Áhættumatskrá símakerfa.pdf“* og *„Viðauki Imatsflokkar og viðmið áhættumats.pdf“.*

(18) Í svari Sýnar, dags. 20. september 2022, kom fram að þann 13. júlí hafi verið framkvæmdar breytingar í miðlægum símakerfabúnaði félagsins sem olli alvarlegu útfalli á þjónustu fyrirtækisins. Breytingarnar höfðu áhrif á fastlínuþjónustu (VoIP og PTSN), stofntenging við fyrirtæki (ISDN, PRI og SUO trunk), farsímaþjónustu, einkasímstöðvaþjónustu Vodafone (OneNet) og samtengingar við önnur fjarskiptafyrirtæki vegna fastlínu og farsímaþjónustu hjá Vodafone.

(19) Í svari félagins kemur fram að „[r]*ofið eða útfallið hafði áhrif á notendur óháð landsvæðum“* og gaf félagið upp eftirfarandi tölulegar upplýsingar:

[...][6]

Mynd 1 sýnir svar Sýnar dags. 20. september 2022 um áhrif útfallsins á notendur.

(20) Þá tiltekur félagið að „[a]*lla jafna er hlutfallslega lítil umferð í farsíma- og fastlínuþjónustu milli kl. 06:00 til 08:00 á morgnanna.“.*

(21) Í svari Sýnar, dags. 16. ágúst 2022, við fyrstu fyrirspurn Fjarskiptastofu og í atvikaskýrslu félagsins vegna öryggisatviksins, kom fram að breytingastjórnunarferlinu hafi ekki verið fylgt með réttum hætti. Fjarskiptastofa óskaði því eftir upplýsingum um verklag við breytingastjórnun ásamt því hvernig hafi verið vikið frá því í umræddum tilviki, sbr. bréf stofnunarinnar dags. 15. september 2022. Í svari Sýnar, dags. 20. september 2022, kom fram að sá aðili sem framkvæmdi breytinguna þann 13. júlí 2022 hafi ekki skráð breytingarnar eins og breytingastjórnarferli félagsins gerir kröfu um. Þar sem breytingarnar voru ekki skráðar var starfsfólk stjórnborð félagsins ekki meðvitað um þær. Í svari Sýnar 20. september kemur ennfremur fram:

> *Einnig voru prófanir og eftirliti eftir breytingar ábótavant hjá þeim framkvæmdi breytinguna sem olli því að afleiðingarnar komu ekki strax í ljós en ef það hefði verið gert hefði það dregið gríðarlega úr þeirri tímalengd sem rofið varði. Ef breytingin hefði verið skráð og prófuð með eðlilegum hætti þá hefði útfallið ekki orðið jafn mikið og það varð.*

(22) Í svari Sýnar, dags. 20. september 2022, kemur fram það mat Sýnar að um var að ræða breytingar sem áður hafi gengið vel og ekki leitt til útfalls á þjónustu og því hefði þessar breytingar sem olli útfalli líklega átt að vera flokkuð sem breyting í minnsta áhættuflokki Sýnar [...][7]

(23) Hvað varðar tilkynningar félagsins til viðskiptavina þann 13. júlí 2022, kemur fram í svari Sýnar að tilkynningar *„*[u]*m rof eða útfall eru sendar til þeirra viðskiptavina sem óska eftir að vera á slíkum tilkynningarlista.“*. Þá segir einnig:

[6] Tafla í bréfinu ekki birt opinberlega.
[7] Efni hluta ákvörðunar ekki birt opinberlega.

Þegar rof eða útfall á þjónustu Vodafone verður eru tilkynningar sem eiga að berast til viðskiptavina skráðar í beiðnakerfið þ.e. í sömu beiðni og atvikið er unnið til að tryggja rekjanleika. Tilkynningar eru sendar ýmist með tölvupósti og/eða sms eftir óskum viðskiptavina.

(24) Þá fylgdu svarinu allar skráðar tilkynningar inn í umræddri beiðni, sbr. *mynd 2*. Kemur þar fram að Sýn áætlaði að senda út fyrstu tilkynninguna klukkan 07:02 þann 13. júlí en fyrir mistök hafi útsending ekki átt sér stað. Upp hafi komist um þau mistök kl. 07:37 og tilkynning um útfall send út þá. Það var svo kl. 07:55 að tilkynning um að viðgerð sé lokið var send út.

[...][8]

Mynd 2 sýnir svar Sýnar við fyrirspurn Fjarskiptastofu um afrit af tilkynningum sem fóru til viðskiptavina þann 13. júlí 2022 vegna öryggisatburðanna.

(25) Þá segir einnig í svari félagsins að „[s]*einna um morguninn þegar vart var við óeðlilega hegðun á fastlínukerfi Vodafone, þar sem tengingar voru óstöðugar á afmörkuðum kerfiseiningum var stofnað nýtt atvik/beiðni kl. 10:27. Strax þá var mótuð tilkynning til viðskiptavina sem skráð er í beiðninni en hún var ekki send út þar sem fastínukerfið var komið í lag kl. 10:35.“*.

2.2 Niðurstaða forskoðunar

(26) 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 Sýnar er varða eftirfarandi:

a. breytingastjórnunarferli,
b. viðhald fjarskiptaneta ásamt stjórnun truflana og bilana,
c. tilkynninga til viðskiptavina og
d. tilkynninga til netöryggissveitarinnar.

(27) Markmið stjórnsýsluskoðunarinnar var að ganga úr skugga um hvort undirbúningur og framkvæmd breytinganna sem olli öryggisatvikinu, sem og viðbrögð við því, hafi verið í samræmi við þær lagakröfur sem á félaginu hvíla skv. 47. gr. þágildandi laga um fjarskipti nr. 81/2003, sbr. einnig ákvæði reglna nr. 1221/2007, um vernd upplýsinga í almennum fjarskiptanetum og reglna nr. 1222/2007, um virkni almennra fjarskiptaneta, sbr. ákvæði I til bráðabirgða í lögum nr. 70/2022, um fjarskipti.

(28) Hvað varðar breytingastjórnun þá byggir þessi niðurstaða stofnunarinnar á svörum Sýnar um að breytingastjórnunin hafi ekki verið fylgt með réttum hætti, sbr. svar Sýnar, dags. 16. ágúst 2022, atvikaskýrslunni og svari Sýnar, dags. 20. september 2022. Í svörum kom m.a. fram að ekki hafi verið gerð breytingastjórnunarbeiðni þó að ferli breytingastjórnunar geri kröfu um það.

[8] Upplýsingar úr innri kerfum Sýnar ekki birt opinberlega.

(29) Þá tók Fjarskiptastofa mið af umfangi þjónusturofa en fyrra þjónusturofið varði í 100 mínútur og segir í svari Sýnar, dags. 20. september, að *„*[e]*f breytingin hefði verið skráð og prófuð með eðlilegum hætti þá hefði útfallið ekki orðið jafn mikið og það varð.“.*

(30) Með hliðsjón af þeim tíma sem tók að endurreisa farskiptaþjónustuna þá vöknuðu spurningar um hvort veikleikar væru í verklagi Sýnar við endurreisn eftir bilanir og var því ákveðið að skoða frekar hvernig er staðið að viðhaldi fjarskiptaneta sem og stjórnun truflana og bilana hjá Sýn.

(31) Í svörum Sýnar, dags. 20. september 2022, kom fram það álit félagsins að hnökrar hafi verið í tilkynningum til viðskiptavina og er því mat Fjarskiptastofu að skoða þyrfti fylgni verklagsins við þær reglur sem gilda um tilkynningar til viðskiptavina.

(32) Þá hafði Fjarskiptastofa fyrst fregnir af málinu í gegnum fjölmiðla en ekki með tilkynningu til netöryggissveitarinnar CERT-ÍS. Með tilliti til alvarleika öryggisatviksins taldi Fjarskiptastofa einnig þarft að skoða fylgni við lagaákvæði sem varðar tilkynningarskyldu öryggisatvika til sveitarinnar, og þar með Fjarskiptastofu.

(33) Með hliðsjón af framangreindu, eðli atviksins og upplýsingum frá Sýn boðaði Fjarskiptastofa, með bréfi, dags. 13. október 2022, að stofnunin myndi hefja stjórnsýsluskoðun á framangreindum afmörkuðum þáttum sem varða stjórnkerfi upplýsingaöryggis hjá Sýn.

III. Lagaumhverfi

(34) 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 og stuðla að öryggi almennings, fyrirtækja og samfélagsins alls á sviði fjarskipta og netöryggis, sbr. 1. og 2. mgr. 3. gr. laga um Fjarskiptastofu.

(35) Þegar öryggisatvikið átti sér stað voru í gildi fjarskiptalög nr. 81/2003 og verður 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. Var hér lögfest inntak upplýsingaöryggis, þ.e. að tryggja skuli leynd upplýsinga, lögmæti aðgangs að þeim og réttleika. Með lögum nr. 78/2019 var fjarskiptalögum nr. 81/2003 svo breytt frekar með því að bæta við skilgreiningu á öryggi net- og upplýsingarkerfa, sbr. 47. tl. 3. gr. laga nr. 81/2003.

(36) 1. og 2. málsgrein 47. gr. laga nr. 81/2003 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].

(37) 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. 1. mgr. ákvæðisins. Þá skal fjarskiptafyrirtæki jafnframt gera sérstakar ráðstafanir til að tryggja samfelldan og órofinn rekstur almennra fjarskiptaneta, sbr. 2. mgr. ákvæðisins. Í sömu málsgreinum er mælt fyrir um að Fjarskiptastofa setji sérstakar reglur um vernd upplýsinga og virkni almennra fjarskiptaneta. Í þessu skyni 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.

(38) 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 á grundvelli áhættumatsins 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 fjarskiptaneta 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.*

(39) Í II. kafla reglna nr. 1222/2007 er að finna almennar kröfur og leiðbeiningar en þar segir í 4. gr. að í reglunum komi fram kröfur til fjarskiptafyrirtækja um að tryggja virkni og öryggi fjarskiptaneta. Þar segir sérstaklega að „[þ]*ær 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.“.*

(40) Í 5. gr. er 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.*

(41) 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.“.*

(42) Þá er einnig 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 náttúruhamfara, 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 mikilvægu 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 Póst- og fjarskiptastofnunar nr. 1221/2007 um vernd upplýsinga í almennum fjarskiptanetum.*

(43) 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.

(44) Í 22. gr. reglna nr. 1222/2007, um virkni almennra fjarskiptaneta er svo fjallað um stjórnun truflana og bilana, en þar segir:

Á grundvelli bilana- og truflanaskýrslna eða tilkynninga frá búnaði, skulu fjarskiptafyrirtæki, á hvaða tíma sólarhringsins sem er, hafa getu til að gera nauðsynlegar ráðstafanir til að gera við bilanir sem valda mikilli truflun á umferð og þjónustu.

Til að reisa fjarskiptanetin við á sem skemmstum tíma, skulu skýrar leiðbeiningar vera til staðar í neyðaráætlun og ábyrgðarsvið hvers og eins vera ljóst, þar með talið nauðsynlegar upplýsingar til að ná í viðgerðarmenn, upplýsingar um varabúnað, skipulag tilkynninga og leiðbeiningar til að vernda neyðarumferð með tímabundnum ráðstöfunum. Í þessum tilgangi skulu þjónustu- og rekstrarborð vera með leiðbeiningar um samvinnu við önnur þjónustu- og rekstrarborð.

Búnaður í fjarskiptanetum skal vera með samstilltar klukkur er auðvelda samvirkni og rekjanleika aðgerða.

Viðhalda skal skrám um bilanir og truflanir sem geta hjálpað til við viðgerð og fyrirbyggjandi viðhaldsaðgerðir og til að rannsaka þjónustugæði og afköst fjarskiptanetanna.

Við stjórnun fjarskiptaneta, skal gera ráð fyrir að hægt verði að tilkynna öðrum fjarskiptafyrirtækjum um mikilvæg tæknileg atriði og truflanir sem hafa áhrif á samtengiumferð milli þeirra.

(45) 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.

(46) 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.

(47) Á grundvelli þess skulu vera til staðar verkferlar sem fjalla um breytingar sem taka til allra breytinga sem geta haft áhrif á fjarskiptanetin og skulu þeir tryggja viðeigandi formlega meðhöndlun breytinga ásamt skjalfestingu þeirra. Verkferlarnir skulu hafa í för með sér traustan, skipulegan og fyrirsjáanlegan rekstur fjarskiptaneta.

(48) Þá skal fjarskiptafyrirtæki samkvæmt 1. mgr. 26. gr. áðurnefndra reglna nr. 1222/2007 tilkynna viðskiptavinum um alvarleg öryggisatvik í fjarskiptanetum. Þjónustuviðmið slíkra tilkynna skulu vera í samræmi við 1. mgr. 24. gr. 1222/2007, en þar segir:

Fjarskiptafyrirtæki skulu vera með skýra og skilvirka ferla vegna tilkynninga um ósamfellda virkni, eða hættu á slíku í almennum fjarskiptanetum sínum, svo sem af völdum truflana, bilana og breytinga. Tilkynna skal viðskiptavinum um slík atvik og skulu þjónustuviðmið þar að lútandi koma fram á heimasíðu fyrirtækisins eða eftir sambærilegum leiðum, t.d. í viðskiptamannasamningum. Í tilkynningunum þarf að lágmarki að koma fram hvaða áhrif atvikið hefur eða getur haft og þær ráðstafanir sem fjarskiptafyrirtækið muni gera, ásamt ráðleggingum til viðskiptamanna ef svo ber undir.

(49) Í 1. mgr. 47. gr. a. laga nr. 81/2003, um fjarskipti er gerð sú krafa til fjarskiptafyrirtækja að þau tilkynna netöryggissveit án tafar um öryggisatvik eða áhættu sem ógnar net- og upplýsingakerfum þeirra.

(50) Eins eru gerðar kröfur um tæknilegar ráðstafanir í 12. gr. reglna nr. 1221/2007, sem fjarskiptafyrirtæki á að viðhafa. Þar kemur sérstaklega fram, sbr. 8. og 9. tl. að þau skuli *„*[V]*iðhalda 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“* sem og *„*[H]*alda skrá um aðgangsheimildir og* aðgangsréttindi *og yfirfara reglulega. Skal fjarskiptabúnaður vera stilltur til samræmis við þá skráningu.“*.

IV.
Stjórnsýsluskoðun Fjarskiptastofu

4.1 Afmörkun stjórnsýsluskoðunar

(51) Líkt og að framan greinir beindist stjórnsýsluskoðun Fjarskiptastofu að öryggisatviki sem átti sér stað þann 13. júlí 2022. Stjórnsýsluskoðunin tók til þeirra þátta í öryggisskipulagi Sýnar sem varða eftirfarandi:

1. viðhald fjarskiptaneta, sbr. 20. gr. reglna nr. 1222/2007,
2. stjórnun truflana og bilana, sbr. 22. gr. reglna nr. 1222/2007,
3. breytingastjórnun, sbr. 23. gr. reglna nr. 1222/2007,
4. tilkynningar um alvarleg öryggisatvik til viðskiptavina, sbr. 1. mgr. 26. gr. og 1. mgr. 24. gr. reglna nr. 1222/2007,
5. tilkynningar til netöryggissveitar, sbr. 47. gr. a. fjarskiptalaga nr. 81/2003.

(52) Fyrstu tveir skoðunarliðirnir, þ.e. viðhald fjarskiptaneta og stjórnun truflana og bilana eru skoðaðir samhliða og er umfjöllun því sameinuð hér eftir.

4.2 Gagnabeiðni Fjarskiptastofu

(53) Með hliðsjón af alvarleika öryggisatviksins vöknuðu spurningar hjá stofnunni um hvernig staðið er að breytingastjórnun og viðhaldi fjarskiptaneta hjá félaginu. Hóf stofnunin stjórnsýsluskoðun á öryggisatvikinu og þeim öryggisatburðum sem urðu í kjölfari þess og var félaginu tilkynnt þar um með bréfi dags. 13. október 2022. Í bréfinu var einnig sett fram upplýsingabeiðni stofnunarinnar en þar var óskað eftirfarandi gagna:

1. *Lýsingu á þeirri breytingu sem síðar olli öryggisatvikum að morgni 13. júlí sl.*
2. *Afriti af nýjustu breytingarstjórnunarbeiðni fyrir sambærilega breytingu og þeirri sem leiddi til umrædds öryggisatviks.*
3. *Hver er skýring þess að umrædd breyting var framkvæmd kl. 06:10 þegar skilgreind tímaviðmið skv. breytingarstjórnunarferli Sýnar er á milli 01:00 og 06:00?*
4. *Hvernig var upplýsingagjöf um breytinguna háttað áður en hún var framkvæmd, þ.e. hverjir voru upplýstir og um hvað?*
5. *Hvaða upplýsingar lágu fyrir um breytinguna og voru aðgengilegar þeim sem verða öryggisatviksins varir kl. 06:30?*
6. *Afriti af afturhvarfsáætlun (e. rollback) breytingarinnar.*
7. *Hvort og hvaða prófanir voru gerðar áður en breytingin var framkvæmd kl. 06:10?*
8. *Skýringu á því að varabúnaður (speglun kerfis) eða önnur úrræði, til að viðhalda samfelldum rekstri, komu ekki í veg fyrir að þjónusturof yrði í kjölfar breytingarinnar sem gerð var kl. 06:10?*
9. *Afriti af niðurstöðum síðustu innri úttekt Sýnar á breytingarstjórnunarferli félagsins.*

(54) Varðandi umfang þjónusturofs þá óskaði Fjarskiptastofa eftir:

10. *Sundurliðun, umfram það sem kemur fram í fyrri svörum Sýnar, á umfangi áhrifa beggja öryggisatvika, þ.e. á hvaða þjónustu atvikin höfðu og fjölda viðskiptavina.*
11. *Tölulegum og myndrænum upplýsingum fyrir notkun fastlínuþjónustu, stofntengingu við fyrirtæki og einkasímstöðvaþjónustu, sambærilegum þeim og afhent hefur verið fyrir notkun á farsímaþjónustuna.*

(55) Varðandi tilkynningar til viðskipavina þá óskaði Fjarskiptastofa eftir:

12. *Afriti af ferli Sýnar vegna tilkynninga um alvarlegra öryggisatvika til viðskiptavina félagsins.*
13. *Tengli á heimasíðu Sýnar þar sem þjónustuviðmið til viðskipavina koma fram.*

4.3 Gögn og upplýsingar frá Sýn

(56) Fjarskiptastofu bárust svör og gögn frá Sýn þann 28. október 2022. 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 niðurstaðna.

4.4 Forsendur niðurstöðu stjórnsýsluskoðunar

4.4.1 Breytingastjórnun

(57) Í gagnabeiðni Fjarskiptastofu frá 13. október 2022 var óskað upplýsinga um hverjar væru orsakir öryggisatviksins þann 13. júlí 2022 og þeirra öryggisatburða sem urðu í kjölfarið. Þá var óskað upplýsinga um þær prófanir sem gerðar voru áður en breyting var framkvæmd í kerfi Sýnar. Í svari félagsins, dags. 27. október 2022, segir:

> *Með breytingunni sem var framkvæmd kl. 06:10 13. júlí síðastliðinn átti að bæta við nýjum forðum á báðum fastlínusímstöðvum þannig að hægt væri að setja upp fleiri SIP trunk tengingar á þeim.*
> *SIP trunk tengingarnar sjálfar átti að setja upp síðar og prófa virkni á þeim.*
> *Breytingin sjálf var í eðli sínu ekki umfangsmikil, þ.e. eingöngu átti að bæta við skilgreiningu á einu porti við fyrirliggjandi uppsetningu (jafnast á við eina línu í kóða).*

(58) Þá segir enn fremur:

> *Prófanir voru ekki framkvæmdar áður en breytingin var framkvæmd kl. 06:10. Prófanir voru ekki framkvæmdar eftir að breytingin var framkvæmd kl 06:10 þar sem starfsmaðurinn sem framkvæmdi breytinguna taldi hana hafa heppnast þar sem ekki komu fram neinar villur í þeim viðmótum sem breytingin var gerð.*

(59) Af gögnum málsins má sjá að Sýn hefur skilgreint verklag fyrir breytingastjórnun. En markmið þess skv. áðurnefndri verklagsreglu félagsins um breytingarstjórnun „*Breytingastjórnunarferli.pdf*“ er eftirfarandi:

> *Markmið breytingastjórnunar er að bregðast skilvirkt við breytingum á kröfum viðskipta og IT. Breytingastjórnun tryggir staðlaðar aðferðir, bætir upplýsingamiðlun og dregur úr áhættu á skertri þjónustu til viðskiptavina vegna breytinga sem framkvæmdar eru.*

(60) Við yfirferð Fjarskiptastofu á gögnum frá Sýn er ljóst að ekki var farið eftir áðurnefndri verklagsreglu félagsins um breytingastjórnun „*Breytingastjórnunarferli.pdf“* þegar kemur að þeim breytingum sem voru framkvæmdar þann 13. júlí 2022.

(61) Má þar í fyrsta lagi nefna að ekki er skráð beiðni fyrir umræddar breytingar líkt og verklag breytingastjórnunar hjá félaginu gerir kröfu um. Sökum þess voru ekki til skráðar upplýsingar hjá félaginu um umræddar breytingar eða lýsingu á framkvæmd þeirra (e. Implementation). Þetta leiddi jafnframt til þess að einungis sá starfsmaður sem framkvæmdi umræddar breytingar hafði vitneskju um þær, þ.e. að þær hafi verið gerðar, hvenær þær voru framkvæmdar o.s.frv.

(62) Í öðru lagi sýna gögn frá Sýn, sbr. bréf Sýnar dags. 27. október 2022, að hvorki voru framkvæmdar prófanir fyrir eða eftir að breytingarnar voru framkvæmdar í fyrri fastlínusímstöðunni né í síðari fastlínusímstöðinni. En verkferill breytingastjórnunar Sýnar tilgreinir að fyrir „standard“ breytingu eigi að framkvæma almennar prófanir skv. lýsingu deilda. Að auki er prófun breytinga viðurkennt verklag um bestu framkvæmd, sbr. 12.1.2 Breytingastjórnun í ÍST EN ISO/IEC 27002:2017. Í svörum félagsins segir að ástæðan fyrir því að ekki var farið í prófanir sú að umræddar breytingar voru taldar hafa heppnast þar sem ekki komu fram villur í þeim viðmótum sem breytingarnar voru gerð á.

(63) Í þriðja lagi að þá er skilgreint í verklagsreglu breytingastjórnunar hjá félaginu á hvaða tíma heimilt er að framkvæma breytingar í kerfum félagsins. [...][9].

(64) Sú breytingin sem hér er til skoðunar og sem olli öryggisatvikinu var gerð 06:10 að morgni miðvikudags og því utan þess tíma sem að heimilt er að framkvæma breytingar. Þótt að almennt sé lítil notkun á fjarskiptaþjónustu Sýnar á þeim tíma sem breytingarnar voru framkvæmdar, er ljóst að hún var ekki í samræmi við breytingastjórnunarferli félagsins hvað þetta varðar. Að áliti Fjarskiptastofu ber að leggja til grundvallar að breytingum sé að jafnaði lokið vel innan þeirra tímamarka sem verklagsreglur kveða á um.

(65) Það er mat Fjarskiptastofu að skjalfest verklag breytingastjórnunar stuðli að góðri breytingastjórnun, ef unnið er eftir því. Breytingarnar sem eru til skoðunar leiddu til þess að rof og truflanir urðu á þjónustu Sýnar í samtals um 180 mínútur, þ.e. fyrst frá 06:10-07:50 og síðar frá 09:15-10:35, sbr. atvikaskýrslu Sýnar, sem varðaði um 200 þúsund notendur en um 7000 notendur urðu fyrir áhrifum, sbr. svarbréf félagsins, dags. 20. september 2022, og athugasemdir frá félaginu, dags. 28. apríl 2023.

(66) Umræddar breytingar voru ekki framkvæmdar í samræmi við samþykkt breytingastjórnunarferli Sýnar. Ekki var gerð breytingabeiðni fyrir umræddar breytingar, breytingarnar voru hvorki prófaðar fyrir né eftir framkvæmd sem og þær voru unnar utan tilgreindra tímamarka fyrir framkvæmd breytinga í kerfum félagsins.

(67) Á grundvelli ofangreinds er það mat Fjarskiptastofu að Sýn hafi ekki uppfyllt kröfur 1. og 2. mgr. 23. gr. reglna nr. 1222/2007 þegar það framkvæmdi breytingar í miðlægum símkerfabúnaði félagsins 13. júlí 2022, þar sem félagið framkvæmdi þær ekki í samræmi við samþykkt breytingastjórnunarferli sitt.

4.4.2 Viðhald fjarskiptaneta ásamt stjórnun truflana og bilana

(68) Líkt og að framan greinir þá er fjallað um viðhald fjarskiptaneta í 20. gr. reglna nr. 1222/2007 og um stjórnun truflana og bilana í 22. gr. reglnanna.

(69) Þær breytingar sem framkvæmdar voru í kerfum Sýnar þann 13. júlí 2022 voru hluti af viðhaldi félagsins á kerfum þess. Í svari Sýnar, dags. 27. október 2022, er rakið hverjar breytingarnar voru og sett fram lýsing á framkvæmd þeirra.

[9] Efni hluta ákvörðunar ekki birt opinberlega.

(70) Þar kemur fram að Sýn hefur tvær fastlínusímstöðvar sem eru í tveimur aðskildum hýsingarsölum sem eru settar upp þannig að þær geta tekið við meginhluta þjónustunnar ef önnur þeirra verður óstarfshæf.

(71) Hvað varðar öryggisatvikið sem til skoðunar eru í stjórnsýslumáli þessu þá var fyrst framkvæmd breyting í annarri fastlínusímstöðinni. Þar sem ekki komu fram villur í kjölfar hennar eða aðrar vísbendingar um annað en að breytingarnar hafi verið árangursríkar voru breytingar í kjölfarið framkvæmdar á hinni fastlínusímstöðinni. Ekki komu heldur fram villur eða vísbendingar um að eitthvað væri að eftir þær breytingar.

(72) Í atvikaskýrslu sem Sýn afhenti Fjarskiptastofu er að finna tímasetta atburðarás. Gefur það nokkuð skýra mynd af viðbrögðum Sýnar við öryggisatvikinu og endurreisn þjónustunnar. Verklagið var á þá leið að bilun uppgötvast 06:30 eða 20 mínútum eftir að breytingarnar á símkerfunum voru framkvæmdar. Það er svo 5 mínútum síðar sem bakvakt er kölluð út og er neyðaráætlun félagsins virkjuð kl. 07:00. Greining og viðgerð hefst strax og er meðal annars kallað eftir aðstoð frá sérfræðingum framleiðanda símkerfanna. Klukkan 07:55 eru símakerfin komin í eðlilegt horf eða 1 klst. og 45 mínútum eftir að breytingarnar voru framkvæmdar.

(73) Bilunar verður þó aftur vart kl. 09:15 en þá við afmarkaðri hluta fastlínukerfisins. Það er svo tíu mínútum síðar sem ástæða seinna öryggisatburðarins greinist, þ.e. að misræmi er í kerfisskilgreiningum en leiðrétting var gerð á þeim klukkan 7:22. Samkvæmt gögnum Sýnar var viðgerð lokið klukkan 10:11 og er það staðfest kl. 10:35 að kerfi virki eðlilega. Það er um 80 mínútum eftir að vart var við seinni bilunina.

(74) Langur endurreisnartími er að mestu leyti vegna þess að viðgerð var tímafrek. Vegur þar þungt að stjórnborð Sýnar hafði ekki skráðar upplýsingar um breytingarnar og hafði einungis sá starfsmaður sem framkvæmdi breytingarnar vitneskju um þær. Umræddur starfsmaður var á bakvakt og kom að úrlausn málsins. Óháð tímalengd aðgerða þá ber atvikaskýrslan með sér að öguðum vinnubrögðum af hálfu Sýn hafi verið beitt við endurreisn þjónustunnar.

(75) Líkt og áður segir voru breytingarnar sem ollu öryggisatvikinu hluti af viðhaldi Sýnar á kerfum sínum. Af viðbrögðum við rofinu, skv. atvikaskýrslu, eru vísbendingar um að unnið hafi verið að því að endurreisa fjarskiptaþjónustuna eins fljótt og auðið var. Það að breytingastjórnunarferli Sýnar hafi ekki verið fylgt leiddi til þess að endurreisnartími er mun lengri en vænta mætti.

(76) Í atvikaskýrslu öryggisatviksins er tilgreint að kl. 06:30 hafi stjórnborð Sýnar fengið villumeldingar úr kerfum auk tilkynninga frá viðskiptavinum um óeðlilega hegðun. Lýsing í skýrslunni ber þess merkis að Sýn hafi haft aðgang að viðeigandi mannauði til að vinna að viðgerð, þar á meðal þjónustu frá framleiðanda símkerfanna.

(77) Sýn hefur, eins og áður hefur komið fram, neyðaráætlun sbr. *„Neyðaráætlun Sýnar.pdf“* sem varðar bilun í búnaði, þar er m.a. að finna viðbragðsáætlun vegna bilana í símstöðvum. Meðal aðgerða stjórnborðs er að afla upplýsinga um atburð og staðsetningu bilana, hafa samband við bakvakt, skrá atvikið í atvikaskrá og senda tilkynningar um rekstrartruflanir til aðila á póstlista.

(78) Þá er það hluti aðgerða bakvaktar símkerfa að meta umfang bilana, vinna að úrlausn máls og hafa samband við framleiðanda. Er tiltekið í viðbragðsáætluninni hvar upplýsingar um framleiðanda séu aðgengilegar. Að auki má sjá gátlista fyrir aðgerðastjóra og yfirlit yfir viðbragðsaðila innan fyrirtækisins, símanúmer og netfang þeirra.

(79) Eftir yfirferð gagna frá Sýn og samanburð á atvikaskýrslu og viðbragðsáætlun er það mat Fjarskiptastofu að starfsmenn Sýnar hafi fylgt framangreindri viðbragðsáætlun þegar upp komu öryggisatvik þann 13. júlí 2022. Það er niðurstaða stofnunarinnar að ferli félagsins og viðbrögð séu í samræmi við 20. gr. og 22. gr. reglna nr. 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.

(80) Fjarskiptastofa vekur þó sérstaklega athygli á 4. mgr. 20 gr. reglna nr. 1222/2007 en þar kveður á um að eftir því sem við á skulu fjarskiptafyrirtæki hafa nægan varabúnað og önnur úrræði til að viðhalda samfelldum rekstri. Af svörum Sýnar má sjá að til staðar eru tvöfalt símkerfi sem gegna hlutverki sem varabúnaður hvors annars, en þar sem breytingar voru gerð í báðum kerfum fóru þau bæði niður. Að mati Fjarskiptastofu var það skortur á hlítni við breytingastjórnunarferli Sýnar sem leiddi til þess að útfall varð á þjónustu félagsins, þ.e. í báðum kerfum þess en ekki skortur á varabúnaði sem slíkum.

4.4.3 Tilkynning til viðskiptavina

(81) Líkt og að framan greinir þá kveður 1. mgr. 26. gr. reglna nr. 1222/2007 á um skyldu fjarskiptafélaga að tilkynna viðskiptavinum um alvarleg öryggisatvik í fjarskiptanetum.

(82) Hvað varðar tilkynningu Sýnar til viðskiptavina sinna þá kemur fram í svörum félagsins, dags. 20. september 2022, og atvikaskýrslu, að fyrirhugað hafi verið að senda fyrstu tilkynningu til viðskiptavina kl. 07:02 þann 13. júlí 2022. Hins vegar hafi útsending tilkynningarinnar ekki heppnast þar sem tegund útfalls við gerð tilkynningar var ekki breytt. Þá var ekki gengið úr skugga um að sending hafi heppnast og viðskiptavinum hafi borist umrædd tilkynning. Enn fremur segir í atvikaskýrslu að „[s]*tjórnborð tekur saman upplýsingar um umfang atviks og tilkynning send út til viðskiptavina.(sem kom síðar í ljós að tilkynning fór ekki út)“.*

(83) Samkvæmt atvikaskýrslu varð það svo kl. 7:39[10] að stjórnborð félagsins áttar sig á að fyrir mistök hafi umrædd tilkynning ekki verið send út líkt og áður var talið og er brugðist við því með útsendingu tilkynningar. Þá er send önnur tilkynning kl. 07:55 þar sem tilkynnt er um að viðgerð sé lokið. Viðskiptavinir eru því fyrst upplýstir um fyrri öryggisatburðinn um 90 mínútum eftir að rof verður á þjónustu eða 70 mínútur eftir að stjórnborð varð bilunarinnar vart. Ekki eru sendar tilkynningar vegna seinni öryggisatburðarins sem, skv. atvikaskýrslu, stjórnborð varð fyrst vart um kl. 09:15. Í svari Sýnar, dags. 20. september 2022, kom fram að ekki var send út tilkynning um truflunina þar sem fastínukerfið var komið í lag kl. 10:35 eða 8 mínútum eftir að atvik/beiðni var skráð hjá Sýn.

(84) Í svörum Sýnar, dags. 20. september 2022, kom fram að tilkynningarnar hafi verið sendar til þeirra aðila sem hafa óskað eftir að fá slíka tilkynningu í tölvupósti og/eða SMS.

[10] Í atvikaskýrslu er tilgreint að kl. 7:39 hafi stjórnborð áttað sig á mistökunum en í svari Sýnar dags. 20. september 2022 stendur kl. 7:37.

(85) Í 1. mgr. 26. gr. reglna nr. 1222/2007 er lögð sú skylda á fjarskiptafyrirtæki að tilkynna viðskiptavinum sínum um alvarleg öryggisatvik í fjarskiptanetum. Segir að þjónustuviðmið vegna slíkra tilkynninga skuli vera í samræmi við 1. mgr. 24. gr. sömu reglna, er fjallar um tilkynningar um ósamfellda virkni. Í 1. mgr. 24. gr. reglnanna er kveðið á um að þjónustuviðmið skuli koma fram á heimasíðu félagsins eða eftir sambærilegum leiðum. Þá segir einnig að í tilkynningum til viðskiptavina skuli að lágmarki koma fram hvaða áhrif atvikið hefur eða getur haft og þær ráðstafanir sem fjarskiptafyrirtækið muni gera, ásamt ráðleggingum til viðskiptamanna ef svo ber undir.

(86) Fjarskiptastofa óskaði eftir að fá upplýsingar á slóð á heimasíðu Sýnar þar sem þjónustuviðmið til viðskiptavina komu fram. Í svari félagsins 27. október 2022 segir að á heimasíðu félagsins, vodafone.is sé að finna skilmála þjónustu þess. Í svari sínu vísar Sýn sérstaklega til 7. gr. I. kafla almennra skilmála félagsins, sem gilda um alla fjarskiptaþjónustu þess. Þar segir m.a.:

> *Vodafone (Sýn hf.) ber ekki ábyrgð á því að fjarskiptasamband rofni um stund. Vodafone (Sýn hf.) mun þó ávallt leitast við að koma á fjarskiptasambandi að nýju sem fyrst og viðhalda gæðum þjónustunnar. Vodafone (Sýn hf.) ábyrgist ekki tjón sem rekja má til sambandsleysis, rofs á fjarskiptum eða annarra truflana sem kunna verða á rekstri fjarskiptanetsins, hvort sem slíkt má rekja til línubilana, bilana í stöðvum eða annarra utanaðkomandi þátta.*

(87) Í neyðaráætlun Sýnar er komið inná tilkynningar til viðskiptavina. Sýn hefur nokkrar viðbragðsáætlanir sem varða ólík atvik. Sú viðbragðsáætlun sem á við öryggisatvikið sem til skoðunar eru í máli þessu er *„6.8 Bilun í símstöðvum“.* Í kaflanum 6.8.2 segir að senda skuli út tilkynningar um rekstrartruflanir á póstlista, þ.e. þá aðila sem óska eftir að taka á móti slíkum tilkynningum.

(88) Virðist verklagið við útsendingu tilkynninga þann 13. júlí 2022 vera í samræmi við framangreint hvað varðar fyrri öryggisatburðinn en ekki var sent út vegna seinni atburðarins þar sem þjónusta var komin á stuttu eftir að beiðni/atvik var skráð.

(89) Ljóst er að Sýn hefur ferla vegna tilkynninga um ósamfellda virkni og nær m.a. neyðaráætlun Sýnar til útsendingu tilkynninga. Ferlarnir kveða hins vegar eingöngu á um að tilkynna skuli þeim aðilum sem óska eftir að taka á móti slíkum tilkynningum. Að auki voru viðskiptavinir á póstlista sem höfðu óskað eftir að taka á móti slíkri tilkynningu sökum mistaka hjá Sýn ekki upplýstir um fyrri öryggisatburðinn fyrr en um 90 mínútum eftir rof verður, ásamt því að viðskiptavinir fengu ekki tilkynningu um seinni öryggisatburðinn. Þá er ljóst að hvorki er fjallað um þjónustuviðmið í almennum skilmálum Sýnar á heimasíðu félagsins né neyðaráætlun, þ.e. hvaða upptímaviðmið Sýn hefur og frávik frá þeim, né heldur hvenær tilkynningarskylda virkjast vegna slíkra frávika. Aftur á móti er ljóst að sú tilkynningarskylda var talin þörf a.m.k. 35 mínútum áður en að tilkynning var send út vegna fyrri öryggisatburðarins.

(90) Það ákvæði sem Sýn vísar til, þ.e. 7. gr. I. kafla almennra skilmála, getur ekki talist uppfylla kröfu um þjónustuviðmið enda er þar einungis fjallað um fyrirvara á mögulegri skaðabótaábyrgð félagsins við þjónusturof. Að mati Fjarskiptastofu er ljóst að hvort tveggja

skortur á þjónustuviðmiði sem og mistök við útsendingu tilkynninga er ekki í samræmi við 1. og 2. málsl. 1. mgr. 24. gr. reglna nr. 1222/2007, sbr. 1. mgr. 26. gr. reglna nr. 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003.

(91) Þá er ljóst af gögnum málsins að Sýn sendi tilkynningu um bilun í símkerfum sínum til hluta af viðskiptavina sinna, þ.e. þeim viðskiptavinum sem hafa óskað eftir að fá slíkar tilkynningar. Að mati Fjarskiptastofu gerir ákvæði 26. gr. reglna nr. 1222/2007 ekki áskilnað um að viðskiptavinir skrái sig á slíkan póstlista hjá félaginu. Um er að ræða ákvæði er varðar öryggi og virkni fjarskiptaþjónustu og því ljóst að félaginu er skylt á grundvelli greinarinnar að upplýsa sérstaklega þegar alvarleg öryggisatvik koma upp í fjarskiptanetum þess. Rof og truflun á þjónustu félagsins í um 180 mínútur sem varðar um 200 þúsund notendur og um 7000 notendur verða fyrir áhrifum af verður ávallt talið alvarlegt. Hlutleysi almennra skilmála félagsins, sem ekki hafa að greina mælanleg þjónustuviðmið, geta ekki leitt til annarrar niðurstöðu.

(92) Á grundvelli ofangreinds er það niðurstaða Fjarskiptastofu að verklag og framkvæmd Sýnar á útsendingu tilkynninga vegna öryggisatviks sem varð í kerfum félagsins þann 13. júlí 2022 sé ekki í samræmi við kröfu 1. mgr. 26. gr. nr. 1222/2007, sbr. ákvæði 47. gr. þágildandi fjarskiptalaga nr. 81/2003, þar sem einungis hluta viðskiptavina, þ.e. þeirra sem höfðu sérstaklega óskað eftir að vera skráðir á póstlista félagsins fyrir slíkar tilkynningar, en ekki öllum viðskiptavinum sem urðu fyrir áhrifum af öryggisatvikinu, var tilkynnt um það.

(93) Að lokum er það mat Fjarskiptastofu, eftir yfirferð á gögnum málsins og efni tilkynninga Sýnar, að efni þeirra uppfylli kröfu lokamálsliðar 1. mgr. 24. gr. reglna nr. 1222/2007, sbr. 1. mgr. 26. gr. reglna 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003, um hvaða upplýsingar skulu að lágmarki koma fram í tilkynningum til viðskiptavina þess, sbr. mynd tvö að framan.

4.4.4 Tilkynning til netöryggissveitar
(94) Líkt og að framan greinir þá kvað 47. gr. a. í þágildandi fjarskiptalögum nr. 81/2003, á um skyldu fjarskiptafélaga að tilkynna netöryggissveit Fjarskiptastofu án tafar um öryggisatvik eða áhættu sem ógnar net- og upplýsingakerfum þeirra.

(95) Fjarskiptastofu bárust fyrst upplýsingar um umrætt öryggisatvik á vefsíðum fjölmiðla, en á vefsvæði RÚV var öryggisatvikinu gerð skil þann 13. júlí 2022. Í framhaldi af því óskaði Fjarskiptastofa eftir upplýsingum um atvikið hjá Sýn og fékk stofnunin senda atvikaskýrslu í kjölfar þeirrar beiðnar. Sýn tilkynnti netöryggissveit Fjarskiptastofu ekki um öryggisatvikið líkt og þágildandi ákvæði fjarskiptalaga kváðu á um. Verður því ekki komist að annarri niðurstöðu en að Sýn hafi brotið gegn ákvæði 1. mgr. 47. gr. a. í þágildandi fjarskiptalögum nr. 81/2003, sbr. b -liður 2. tl. 30. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða.

V.
Niðurstaða Fjarskiptastofu

5.1 Almennt

(96) Með bréfi, dags. 29. mars 2023, boðaði Fjarskiptastofa fyrirhugaða ákvörðun sína vegna umrædds öryggisatviks, en þar voru forsendur og fyrirhuguð niðurstaða stofnunarinnar reifuð. Með bréfi, dags. 28. apríl 2023, barst Fjarskiptastofu athugasemdir frá Sýn vegna boðaðrar ákvörðunar stofnunarinnar.

(97) Fjarskiptastofa hefur yfirfarið allar athugasemdir sem Sýn setti fram við boðaða niðurstöðu stofnunarinnar. Fallist hefur verið á athugasemdir félagsins um umfang áhrifa öryggisatviksins og hefur orðalag verið uppfært til samræmis við þær athugasemdir sem fram komu í bréfi félagsins, dags. 28. apríl sl. En með framangreindu bréfi Sýnar var bætt við þeim upplýsingum sem veittar voru stofnuninni með bréfi, dags. 20. september 2022, en þar kom fram að atvikið hafi haft áhrif á yfir 200 þúsund notendur. Í bréfi Sýnar, dags. 28. apríl, segir að gera verði greinarmun á þeim notendum sem „urðu fyrir áhrifum“ og þeim sem „gátu orðið fyrir áhrifum“. Í bréfinu kemur svo fram hversu margir notendur hafi að jafnaði verið að nota umrædda þjónustu á þeim tíma sem öryggisatburðirnir átti sér stað, en það eru samanlagt um 7000 notendur skv. upplýsingum félagsins. Verður því miðað við það í þessari ákvörðun að atvikið hafi varðað allt að 200 þúsund notendur en um 7000 notendur orðið fyrir áhrifum. Fjarskiptastofa vill þó vekja athygli á því að þó umfang öryggisatviksins í þessari ákvörðun verði að hluta miðað við meðaltalsnotkun umræddrar þjónustu þá er ekkert í gögnum málsins sem útilokar það að notkunin á þeim tíma sem um ræðir hafi verið önnur og jafnvel mun hærri.

(98) Í bréfi Sýnar, dags. 28. apríl sl., ber félagið fyrir sig að umrætt atvik teljist ekki til öryggisatviks, og að það teljist ekki til breytinga í kerfum félagsins þar sem um viðhald hafi verið að ræða. Fjarskiptastofa telur tilefni til að bregðast við þessum athugasemdum og verður fjallað um þær hér að neðan.

5.2 Öryggisatvik

(99) Í bréfi Sýnar, dags. 28. apríl 2023, ber félagið fyrir sig að umrætt atvik teljist ekki til öryggisatviks í skilningi 49. tl. 3. gr. þágildandi laga nr. 81/2003 og 3. gr. reglna nr. 1222/2007, þar sem umrætt rof og truflun á þjónustu félagsins hafi haft óveruleg áhrif og engum rekstraþáttum stofnað í hættu, auk þess sem upplýsingaröryggi hafi ekki verið ógnað. Í framangreindu bréfi Sýnar segir m.a.:

> *Í ljósi þess hve útfallið hafði óveruleg áhrif var engum rekstrarþáttum í reynd stofnað í hættu, en það er annað af tveim hugtakaskilyrðum þess að um öryggisatvik í skilningi laga 81/2003 hafi verið að ræða. Rekstarsamfella fjarskiptanetsins í heild var að fullu tryggð. Þá var upplýsingaöryggi alls ekki ógnað, en það er síðara hugtakaskilyrði öryggisatviks, sbr. 49. tl. 1. mgr. 3. gr. þágildandi fjarskiptalaga.*

(100) Svo segir einnig eftirfarandi í bréfinu:

> *Þá skortir á að greint sé frá með hvaða hætti atvik málsins eru í andstöðu við 47. gr. Verndarandlag 47. gr. þágildandi fjarskiptalaga er í grunninn upplýsingaöryggi. Þannig segi í 1. mgr. að gera skuli ráðstafanir til að „tryggja öryggi þjónustunnar“ og „verja upplýsingarnar sem fara um fjarskiptanet.“ Einungis ef sérstök hætta er á að leynd fjarskipta á tilteknu fjarskiptaneti verði rofin skal þjónustuveitandi upplýsa um áskrifendur um hættuna. Í máli þessu var fjarskiptaleynd eða upplýsingaöryggi aldrei stofnaði í hættu og því engin sérstök ástæða til að tilkynna áskrifendum um*

slíkt. Þaðan af síður var umfangið slíkt að rekstarsamfellu var hætta búin. Meðal annars af þessum ástæðum uppfyllir atvikið ekki heldur hugtakaskilgreiningu öryggisatviks, sbr. hér að framan.

(101) 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 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.

(102) 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.

(103) Hér að neðan verður fyrst farið yfir það hvort talsverðar líkur hafi verið á því að rekstrarþáttum hafi verið stofnaði í hættu vegna atviksins, síðan hvort upplýsingaöryggi hafi verið ógnað vegna þess og loks hvort atvikið hafi haft skaðleg áhrif á öryggi net- og upplýsingakerfa.

(104) Skilgreining á hugtakinu „öryggisatvik“ í framangreindum réttarheimildum gerir einungis ráð fyrir að talsverðar líkur þurfi að vera á því að rekstarþáttum sé stofnað í hættu. Óumdeilt er að rof og truflun varð á þjónustu félagsins vegna umræddsatviks sem varðaði um 200 þúsund notendur en um 7000 notendur urðu fyrir áhrifum, sem svo leiddi til sérstakra aðgerða af hálfu félagsins til að koma þjónustu á ný. Einnig er óumdeilt að fjarskiptaþjónusta, sem sannarlega er einn veigamesti rekstrarþáttur félagsins, féll niður að hluta sökum rofs og truflana á þjónustu félagsins. Verður í þessu samhengi jafnframt að horfa til þess að verndarandlag þágildandi 47. gr. fjarskiptalaga varðar einmitt öryggi fjarskiptaþjónustu og fjarskiptaneta. Verður því ávallt að skýra það hvort rekstraþáttum sé stofnað í hættu innan marka þess. Er því með engum hætti hægt að setja það í samhengi við rekstur Sýnar hf. með heildstæðum hætti. Það er því mat Fjarskiptastofu að rekstrarþáttum hafi eðli máls samkvæmt verið stofnað í hættu, eða a.m.k. talsverðar líkur hafi verið á því, þar sem fjarskiptaþjónusta féll niður að hluta sökum rofs og truflana á þjónustu félagsins.

(105) 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 stjórnskipulagi 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.*[11] *Það getur auk þess falið í sér aðra eiginleika, svo sem ósvikni, ábyrgni, óhrekjanleika og áreiðanleika.“.*

(106) 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.

(107) 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.

(108) Af framangreindum ástæðum er það mat Fjarskiptastofu að umrætt rof og truflanir sem urðu á þjónustu Sýn hafi varðað upplýsingaöryggi, þar sem tiltækileiki upplýsinga í viðkomandi fjarskiptaneti féll niður og varð fyrir truflunum sem hafði áhrif á virkni kerfisins.

(109) Eins og fram hefur komið þá telst hugtakið „öryggisatvik“ skv. 49. tl. 3. gr. þágildandi fjarskiptalaga nr. 81/2003 einnig vera atvik í skilningi 1. tl. 6. gr. laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða. Skv. 1. tl. 6. gr. laga nr. 78/2019 telst hugtakið „atvik“ vera hver sá atburður sem hefur skaðleg áhrif á öryggi net- og upplýsingakerfa. Í greinargerð með frumvarpi til laga um öryggi net- og upplýsingakerfa mikilvægra innviða er fjallað um 6. gr., en þar segir að „[g]*era má ráð fyrir að árás/innbrot í kerfi, gagnaleki og gagnatap, óvænt stöðvun í rekstri kerfa (í heild eða að hluta)*[12] *og önnur sambærileg tilvik sem hafa áhrif á starfsemi hlutaðeigandi falli hér undir.“*. Þar sem óumdeilt er að rof og truflun varð á þjónustu Sýnar vegna umrædds atviks sem leiddi m.a. til óvæntrar stöðvunar í rekstri kerfa félagsins, sem varðaði um 200 þúsund notendur en um 7000 notendur urðu fyrir áhrifum, þá er það mat Fjarskiptastofu að umrætt atvik hafa haft skaðleg áhrif á öryggi net- og upplýsingakerfa félagsins.

(110) Af framangreindum ástæðum þá hafnar Fjarskiptastofa andmælum Sýnar að umrætt atvik hafi ekki verið öryggisatvik. Er það mat stofnunarinnar að með umræddu rofi og truflunum á þjónustu félagsins hafi bæði rekstrarþáttum verið stofnað í hættu, eða a.m.k. talsverðar líkur hafi verið á því, auk þess sem upplýsingaöryggi hafi verið ógnað jafnframt því sem atburðirnir höfðu skaðleg áhrif á öryggi net- og upplýsingakerfa félagsins. Þar af leiðandi hafi umrætt atvik verið öryggisatvik í skilningi 49. tl. 3. gr. þágildandi fjarskiptalaga nr. 81/2003, 3. gr. reglna nr. 1222/2007 og 3. gr. reglna nr. 1221/2007.

5.3 Breytingastjórnun

(111) Í bréfi Sýnar, dags. 28. apríl 2023, ber félagið einnig fyrir sig að umrætt öryggisatvik teljist ekki til breytinga í kerfum félagsins þar sem um viðhald hafi verið um að ræða og af þeim ástæðum þá eigi ákvæði 23. gr. reglna nr. 1222/2007 ekki við um atvikið. Í framangreindu bréfi Sýnar segir m.a.:

[11] Undirstrikun Fjarskiptastofu.
[12] Undirstrikun Fjarskiptastofu.

Þá gerir Sýn athugasemdir við að í hinni boðuðu ákvörðun virðist byggt á að í grunninn hafi verið að gera breytingar á kerfum félagsins. Það er ekki alls kostar rétt, heldur var um viðhald að ræða, sem hafði þær afleiðar að útfallið varð. Skiptir þetta verulegu máli þegar kemur að lagagrundvelli hinnar boðuðu ákvörðunar.

(112) Svo segir eftirfarandi í bréfinu:

Þessu utan byggir hin boðaða ákvörðun að miklu leyti á að ekki hafi verið fylgt breytingarstjórnunarferli, sbr. 23. gr. reglna nr. 1222/2007. Um viðhald fjarskiptaneta er hins vegar fjallaði í 20. gr. reglnanna, og um stjórnun truflana og bilana í 22. gr. reglnanna. Raunar kemur þetta fram í hinni boðuðu ákvörðun í kafla 4.4.2. Engu að síður byggir hin boðaða að miklu leyti á 23. gr. reglnanna sem er þó ekki viðhlítandi lagagrundvöllur þegar um viðhald er að ræða. Einnig af þessari ástæðu getur félagið ekki hafa brotið gegn umræddri 23. gr.

(113) Þau gögn sem Fjarskiptastofu hefur borist frá Sýn bera skýrlega með sér að félagið hefur metið það sjálft að umrætt öryggisatvik hafi komið til vegna breytinga í kerfum félagsins og að breytingastjórnun hafi ekki verið framkvæmd með réttum hætti, en í niðurstöðukafla atvikaskýrslu Sýnar segir:

- Breytingar sem voru gerðar í báðum kjarnaeiningum fastlínukerfa Vodafone kl. 06:10 höfðu óvæntar afleiðingar í för með sér en samskonar breytingar hafa verið gerðar nokkrum sinnum áður án þess að upp hafi komið vandamál.
- Breytingarstjórnunarferli var ekki fylgt með réttum hætti sem hafði veruleg áhrif á því hvernig að atvikið átti sér stað og hvaða áhrif málið hafði á þjónustu viðskiptavina.

(114) Í bréfi Sýnar, dags. 16. ágúst 2022, kom einnig fram að öryggisatvikið átti sér stað eftir að breytingar voru gerðar í miðlægum símkerfabúnaði félagsins. Í bréf Sýnar, dags. 20. september 2022, kemur svo fram að þann 13. júlí 2022 hafi verið framkvæmdar breytingar í miðlægum símakerfabúnaði félagsins sem olli alvarlegu útfalli á þjónustu fyrirtækisins.

(115) Sýn hefur einnig skjalfesta verklagsreglu um breytingastjórnunarferlið, sbr.: skjalið *„Breytingastjórnunarferli.pdf.“*. Í skjalinu er tilgreint eftirfarandi markmið:

Markmið breytingastjórnunar er að bregðast skilvirkt við breytingum á kröfum viðskipta og IT. Breytingastjórnun tryggir staðlaðar aðferðir, bætir upplýsingamiðlun og dregur úr áhættu á skertri þjónustu til viðskiptavina vegna breytinga sem framkvæmdar eru.

(116) Þá er þar einnig að finna skilgreiningu á því hvað telst vera breyting og til hvaða breytinga ferlið nær til, en þar segir:

[...][13]

[13] Efni hluta verklagsreglnanna ekki birt opinberlega.

(117) Samkvæmt öllu framangreindu hefur Sýn sjálft metið það með þeim hætti að umrætt öryggisatvik hafi komið til við framkvæmd breytinga í kerfum félagsins sem ekki voru framkvæmdar með réttum hætti. Þess skal einnig getið að eðli máls samkvæmt þá geta breytingar í kerfum falið í sér viðhald, t.d. ef verið er að uppfæra kerfi. Hugtökin „breyting“ og „viðhald“ eru því ekki ósamrýmaleg enda ljóst að til að viðhalda kerfum þarf alla jafna að framkvæma breytingar á þeim, en um slíkar breytingar þarf að fara að þeim kröfum sem kveðið er á um í 23. gr. reglna nr. 1222/2007. Fjarskiptastofa hafnar því þeim andmælum Sýnar að ákvæði 23. gr. reglna nr. 1222/2007 eigi ekki við um umrætt öryggisatvik og er það jafnframt mat Fjarskiptastofu að þær breytingar sem framkvæmdar voru í kerfum Sýnar þann 13. júlí 2022 hafi verið hluti af viðhaldi félagsins á kerfum þess.

5.4 Niðurstöður

(118) Hér að framan hefur verið gerð grein fyrir þeim álitamálum sem Fjarskiptastofa telur að hafi komið upp vegna öryggisatviks sem átti sér stað í símkerfi Sýnar þann 13. júlí 2022.

(119) Að mati Fjarskiptastofu leiðir stjórnsýsluskoðun stofnunarinnar í ljós ákveðinn veikleika í öryggisskipulagi Sýnar við að tryggja að unnið sé eftir samþykktu breytingaferli félagsins.

(120) Lýsti þessi veikleiki sér í því að breytingar sem Sýn gerði á miðlægum símkerfabúnaði 13. júlí 2022 voru ekki framkvæmdar í samræmi við samþykkt breytingastjórnunarferli félagsins. Ekki var gerð breytingarbeiðni fyrir umræddar breytingar, breytingarnar voru hvorki prófaðar fyrir né eftir framkvæmd sem og þær voru unnar utan tilgreindra tímamarka fyrir framkvæmd breytinga í kerfum félagsins.

(121) Afleiðingar framangreinds veikleika í öryggisskipulagi Sýnar voru alvarlegt rof og truflun á fastlínuþjónustu og farsímaþjónustu fyrirtækisins og löng bilanagreining og þar af leiðandi langt þjónusturof og truflanir, þ.e. í um 180 mínútur sem varðaði um 200 þúsund notendur en um 7000 notendur urðu fyrir áhrifum.

(122) Það er mat Fjarskiptastofu að Sýn hafi ekki framkvæmt breytingar í miðlægum símkerfabúnaði 13. júlí 2022 í samræmi við samþykkt breytingastjórnunarferli félagsins og þar með hafi framkvæmd breytinganna ekki verið í samræmi við 1. og 2. mgr. 23. gr. reglna nr. 1222/2007.

(123) Það er hins vegar mat Fjarskiptastofu að eftir að öryggisatvikið kom upp hafi starfsmenn Sýnar fylgt viðbragðsáætlun félagsins. Það er því niðurstaða stofnunarinnar að ferli félagsins og viðbrögð við öryggisatvikinu séu í samræmi við ákvæði 20. og 22. gr. reglna nr. 1222/2007.

(124) Stjórnsýsluskoðun Fjarskiptastofu leiddi einnig í ljós ósamræmi við tilkynningarskyldu félagsins til viðskiptavina þess. Þar sem umrætt öryggisatvik leiddi til alvarlegs rofs og truflunar á fastlínuþjónustu og farsímaþjónustu fyrirtækisins og langrar bilanagreiningar og þar af leiðandi langs þjónusturofs og truflana, þ.e. í um 180 mínútur sem varðaði um 200 þúsund notendur en um 7000 notendur urðu fyrir áhrifum, er það mat Fjarskiptastofu að um alvarlegt öryggisatvik sé að ræða sem Sýn hafi verið skylt að tilkynna til viðskiptavina sinna í samræmi við 1. mgr. 26. gr. reglna nr. 1222/2007.

(125) Fyrri öryggisatburðurinn átti sér stað kl. 06:10. Fram kemur í svörum Sýnar að fyrirhugað hafi verið að senda tilkynningu, til þeirra aðila sem höfðu óskað eftir að fá slíka tilkynningu í tölvupósti og/eða SMS, kl. 07:02 þann 13. júlí 2022 en fyrir mistök hafi útsending ekki átt sér stað fyrr en kl. 7:39[14]. Þá er send önnur tilkynning kl. 07:55 þar sem tilkynnt er um að viðgerð sé lokið. Viðskiptavinir eru því ekki upplýstir um fyrri öryggisatburðinn fyrr en um 90 mínútum eftir að rof verður á þjónustu og 70 mínútur eftir að stjórnborð varð bilunarinnar vart. Ekki er send tilkynning vegna seinni öryggisatburðarins.

(126) Það er ljóst af gögnum málsins að Sýn sendi tilkynningu um bilun í símkerfum sínum til einungis hluta viðskiptavina sinna, þ.e. þeim viðskiptavinum sem höfðu óskað eftir að fá slíkar tilkynningar. Að mati Fjarskiptastofu gerir ákvæði 1. mgr. 26. gr. reglna nr. 1222/2007 ekki áskilnað um að viðskiptavinir skrái sig á slíkan póstlista hjá félaginu. Um er að ræða ákvæði er varðar öryggi og virkni fjarskiptaþjónustu og því ljóst að félaginu er skylt á grundvelli greinarinnar að upplýsa alla viðskiptavini þegar alvarleg öryggisatvik koma upp í fjarskiptanetum þess. Þar sem það var ekki gert er það því mat Fjarskiptastofu að Sýn hafi brotið gegn 1. mgr. 26. gr. reglna nr. 1222/2007.

(127) Ljóst er að Sýn hefur ferla vegna tilkynninga um ósamfellda virkni og nær m.a. neyðaráætlun Sýnar til útsendingu tilkynninga. Aftur á móti kemur þar eingöngu fram að send skuli tilkynning til þeirra aðila sem óska eftir að taka á móti slíkum tilkynningum. Þá er ljóst að hvorki er fjallað um þjónustuviðmið í almennum skilmálum Sýnar á heimasíðu félagsins né neyðaráætlun, þ.e. hvaða upptímaviðmið Sýn hefur og frávik frá þeim né heldur hvenær tilkynningarskylda virkjast vegna slíkra frávika. Það er því mat Fjarskiptastofu að ferlar Sýnar vegna tilkynninga um ósamfellda virkni, eða hættu á slíku í almennum fjarskiptanetum sínum, og þjónustuviðmið tilkynninga til viðskiptavina um slík atvik sem fram eiga að koma á heimasíðu fyrirtækisins eða eftir sambærilegum leiðum séu ekki í samræmi við 1. og 2. málsl. 1. mgr. 24. gr. reglna nr. 1222/2007.

(128) Líkt og fram hefur komið er það mat Fjarskiptastofu að umrætt öryggisatvik sé alvarlegt. Af því leiðir að það var tilkynningarskylt til netöryggissveitar Fjarskiptastofu skv. 1. málsl. 1. mgr. 47. gr. a. þáverandi fjarskiptalaga nr. 81/2003. Þar sem Sýn tilkynnti ekki án tafar um öryggisatvikið til netöryggissveitar Fjarskiptastofu þá er það mat stofnunarinnar að Sýn hafi brotið gegn 1. málsl. 1. mgr. 47. gr. a. þágildandi fjarskiptalaga nr. 81/2003.

(129) Atvik þessa máls áttu sér stað í tíð þáverandi fjarskiptalaga nr. 81/2003, en skv. þeim lögum er ekki heimild til álagningar stjórnvaldssekta vegna umræddra brota. Kemur því ekki til álita að leggja á Sýn stjórnvaldssekt í þessari ákvörðun. Fjarskiptastofa vill þó vekja athygli á því að hefðu atvik máls átt sér stað eftir að gildandi fjarskiptalög nr. 70/2022 tóku gildi 1. september 2022, þá hefði komið til álita að leggja á félagið stjórnvaldssekt, sbr. heimild í l. lið 1. mgr. 103. gr. þeirra laga, einkum vegna vanrækslu Sýnar á því að uppfylla tilkynningarskyldu sína til netöryggissveitar Fjarskiptastofu.

[14] Í atvikaskýrslu er tilgreint að kl. 7:39 hafi stjórnborð áttað sig á mistökunum en í svari Sýnar dags. 20. september 2022 stendur kl. 7:37.

Á k v ö r ð u n a r o r ð

1. **Framkvæmd breytinga í kerfum Sýnar hf. kl. 06:10 þann 13. júlí 2022 var ekki í samræmi við kröfur 1. og 2. mgr. 23. gr. reglna nr. 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003, sbr. ákvæði I til bráðabirgða við lög nr. 70/2022.**

2. **Framkvæmd Sýnar hf. á tilkynningum til viðskiptavina vegna öryggisatviks sem kom upp við framkvæmd breytinga í kerfum Sýnar hf. sem gerðar voru kl. 06:10 þann 13. júlí 2022 var ekki samræmi við 1. mgr. 24. gr. reglna nr. 1222/2007, sbr. 1. mgr. 26. gr. reglna nr. 1222/2007, sbr. 47. gr. þágildandi fjarskiptalaga nr. 81/2003, sbr. ákvæði I til bráðabirgða við lög nr. 70/2022.**

3. **Verklag og framkvæmd Sýnar hf. á útsendingu tilkynninga til viðskiptavina vegna öryggisatviks sem kom upp við framkvæmd breytinga í kerfum Sýnar hf. sem gerðar voru kl. 06:10 þann 13. júlí 2022 var ekki í samræmi við kröfu 1. mgr. 26. gr. reglna nr. 1222/2007, sbr. ákvæði 47. gr. þágildandi fjarskiptalaga nr. 81/2003, sbr. ákvæði I til bráðabirgða við lög nr. 70/2022, þar sem einungis hluta viðskiptavina var tilkynnt um öryggisatvikið.**

4. **Sýn hf. braut gegn ákvæði 1. málsl. 1. mgr. 47. gr. a. í þágildandi fjarskiptalögum nr. 81/2003, sbr. b lið 2. tl. 30. gr. laga nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða, með því að tilkynna ekki án tafar um öryggisatvik sem kom upp við framkvæmd breytinga í kerfum Sýnar hf. sem gerðar voru kl. 06:10 þann 13. júlí 2022.**

5. **Ákvörðun þessi er kæranleg til úrskurðarnefndar fjarskipta- og póstmála, sbr. 20. gr. laga nr. 75/2021 um Fjarskiptastofu. Kæran skal berast úrskurðarnefnd innan fjögurra vikna frá því viðkomandi var kunnugt um ákvörðun Fjarskiptastofu. Um kostnað vegna málskots fer samkvæmt 5. mgr. 20. gr. sömu laga, auk þess sem greiða ber sérstakt málskotsgjald að upphæð kr. 150.000, skv. 6. gr. reglugerðar nr. 36/2009 um úrskurðarnefnd fjarskipta- og póstmála. Samkvæmt lögum nr. 75/2021 um Fjarskiptastofu getur aðili einnig borið ákvörðun stofnunarinnar beint undir dómstóla án þess að mál sé fyrst borið undir úrskurðarnefnd. Slíkt mál skal höfðað innan þriggja mánaða frá því að viðkomandi fékk vitneskju um ákvörðun stofnunarinnar. Málskot frestar ekki réttaráhrifum ákvarðana stofnunarinnar. Málskot beint til dómstóla hindrar að úrskurðarnefnd sé heimilt að taka kæru til málsmeðferðar.**

Fjarskiptastofa, 22. júní 2023

_____

Hrafnkell V. Gíslason

_____

Björn Þór Rögnvaldsson