Netárás á Vodafone

Skýrsla CERT-ÍS

Netöryggissveit

Póst- og fjarskiptastofnunar

Mars 2014

Inngangur

Laust eftir miðnætti þann 30. nóvember, 2013 voru vefsíður Vodafone á Íslandi eyðilagðar, meðal annars þjónustusíður fyrirtækisins, og markaði það enda innbrots á vefþjóna fyrirtækisins. Stuttu síðar var miklu af viðkvæmum gögnum lekið á netið sem stolið hafði verið í því innbroti.

Hér á eftir er skýrsla Netöryggissveitar Póst- og fjarskiptastofnunar um málið, en nægjanlegur tími er nú liðinn frá atvikinu til að meta megi viðbrögðin af yfirvegun. Fyrri hluti skýrslunnar lýsir viðbrögðum og aðgerðum CERT-ÍS og PFS, en seinni hlutinn fjallar um hvaða lærdóma má draga af viðbrögðum CERT-ÍS og leggur til úrbætur þar að lútandi.

Skýrsla þessi fjallar um aðgerðir og viðbrögð netöryggissveitarinnar CERT-ÍS á grundvelli 47. gr. a., auk reglugerðar nr. 475/2013 um málefni CERT-ÍS netöryggissveittar, þann 30. nóvember 2013 og næstu daga þar á eftir, en ekki álitamálum sem tengjast öðrum ákvæðum laga um fjarskipti nr. 81/2003. Fjallar þessi skýrsla þannig hvorki um það hvort öryggisviðbúnaður í vefkerfi Vodafone hafi verið fullnægjandi og í samræmi við lög né hvort varðveisla þeirra upplýsinga sem stolið var úr vefkerfinu hafi verið heimil lögum samkvæmt. Frumkvæðisrannsókn Póst- og fjarskiptastofnunar og meðferð einstakra kvartana þar að lútandi fer fram í sjálfstæðum stjórnsýslumálum, að hluta til einnig hjá Persónuvernd. Þá vinnur Póst- og fjarskiptastofnun auk þess að heildstæðri úttekt á verklagsreglum farsímafyrirtækjanna um meðferð og eyðingu á fjarskiptaumferðarupplýsingum, en sú úttekt er heldur ekki hluti af skýrslu þessari.

Helstu niðurstöður

Í atvikinu reyndi í fyrsta sinn á skipulag, þekkingu og reynslu netöryggissveitarinnar við að meðhöndla stór öryggisatvik undir tímapressu. Strax og sveitin var orðin meðvituð um atvikið voru viðeigandi verkferlar virkjaðir og unnið eftir þeim í gegnum allt atvikið. Á heildina litið virkuðu verkferlar netöryggissveitarinnar að mestu í samræmi við fyrirætlanir. Fjölmörg atriði komu þó í ljós sem lagfæra þarf; í starfi sveitarinnar, lagaumhverfinu og í samskiptum við ytri aðila.

Þegar starfsmenn CERT-ÍS voru kallaðir út var nokkuð liðið frá því að innbrotið uppgötvaðist, eða um 11 klukkustundir. Nauðsynlegt er að gera viðeigandi breytingar á fyrirkomulagi tilkynninga til sveitarinnar og starfstíma hennar svo stytta megi verulega þennan tíma.

Þegar atvikið er rýnt er ljóst að bæta þarf öflun og miðlun upplýsinga um yfirstandandi atvik þar sem miðlun slíkra upplýsinga innan þjónustuhópsins er ein helsta og áhrifamesta aðgerðin sem sveitin hefur á sínu valdi. Án slíkra upplýsinga eru aðrir aðilar í mikilli óvissu um öryggi þeirra eigin kerfa og verða því óhjákvæmilega að eyða orku í mögulegan óþarfa viðbúnað.

Atvik þetta og afleiðingar þess eru alvarlegar fyrir þá sem hafa orðið fyrir tjóni af völdum þess, beint eða óbeint. Með tilliti til netöryggis við stærri áföll reyndi þetta atvik þó ekki mikið á samhæfingarhlutverk sveitarinnar þótt hún hefði nægum öðrum verkefnum að sinna. Því verður að telja að geta sveitarinnar til að sinna útbreiddari atvikum er takmörkuð af núverandi stærð hennar.

Helsti tilgangur og eðli netöryggissveita á borð við CERT-ÍS er að styðja þjónustuhópinn við að takast á við ógnir og öryggisatvik og því er mikilvægt að draga lærdóm af slíkum atvikum, bæði því sem vel gekk og það sem má bæta.

Fyrsti hluti: Viðbrögð CERT-ÍS og PFS

Kerfi Vodafone og Innbrotið – Almennt yfirlit

Lýsing á innbroti í vefkerfi Vodafone byggir ekki á beinni greiningu CERT-ÍS á viðeigandi kerfum, heldur styðst við skýrslur unnar fyrir Vodafone. CERT-ÍS hefur ekki sannreynt réttleika þessara gagna.

Þau vefkerfi Vodafone sem um ræðir samanstanda af ytri vefþjóni og tengdum gagnagrunni. Aðdragandi innbrotsins virðist hafa verið með þeim hætti að ytri vefþjónninn var skannaður [...][1] með ýmsum aðferðum, í þeim tilgangi að finna veikleika sem síðan væri hægt að nota til að brjótast inn á vefþjóninn. Slíkur veikleiki fannst, sem gerði tölvuþrjótinum kleift að hlaða upp „bakdyrum[2]“ inn á vefþjóninn það sama kvöld. Þetta veitti honum nánast fullkominn aðgang að þjóninum og þeim tengingum sem hann hafði við tengda gagnagrunninn. Veikleikinn sem um ræðir er svokallaður „upload-execute“ veikleiki og kemur til vegna forritunarvillu í sérsniðnu vefkerfi Vodafone.

Afleiðingar þessa aðgangs var sá að tölvuþrjóturinn gat náð í afrit af gögnum úr gagnagrunni tengdum vefkerfinu og síðan reynt að eyða slóð sinni og eyðileggja vefsíður Vodafone aðfaranótt 30. nóvember. Nokkrum klukkustundum seinna dreifði þessi aðili (eða aðilar) gögnum sem stolið var frá Vodafone á hinu almenna interneti og auglýstu það á Twitter.

Tilkynningar og vitneskja

Laugardaginn 30. nóvember 2013, barst vitneskja um netöryggisatvik hjá Vodafone til PFS og CERT-ÍS eftir nokkrum leiðum.

Kl. 02:13 barst tölvupóstur frá *þriðja aðila* beint til starfsmanns CERT-ÍS þar sem greint var frá því að vefsíða Vodafone hefði verið afskræmd. Viðkomandi netfang starfsmannsins er ekki vaktað allan sólarhringinn eða um helgar.

Kl. 08:27 barst tölvupóstur frá [...] Vodafone þar sem tilkynnt var um að brotist hefði verið inn á vefþjón fyrirtækisins og verið væri að vinna í málinu. Viðkomandi netfang (cert@cert.is) hefur ekki sólarhrings- eða helgarvakt.

Kl. 12:19 barst símhringing frá [...] Vodafone í yfirmann tæknideildar PFS (og þar með CERT-ÍS) þar sem tilkynnt var um innbrotið, hvaða upplýsingar (SMS sem send hafi verið af mínum síðum á netinu ásamt lykilorðum) hafi verið sóttar og birtar á netinu. Búið væri að kalla til sérfræðiteymi [...]. Yfirmaður tæknideildar PFS sagðist myndi kalla til netöryggissveit PFS.

Um svipað leyti höfðu starfsmenn PFS og CERT-ÍS vitneskju um málið úr fjölmiðlum, sem og önnur fjarskiptafyrirtæki.

Útkall og mönnun

Í kjölfar þess að starfsmenn PFS urðu meðvitaðir um málið voru starfsmenn CERT-ÍS kallaðir út, þar með talið tveir sérfræðingar CERT-ÍS og forstjóri PFS. Hópstjóri CERT-ÍS var á þessum tíma erlendis vegna vinnu, en var í símsambandi eftir þörfum. Sömuleiðis var yfirmaður tæknideildar PFS utan Reykjavíkur yfir helgina en í símasambandi vegna málsins. Svo vildi til að starfsmaður lögfræðideildar var við vinnu og var hann fenginn til aðstoðar í tengslum við lögfræðileg atriði er lutu að meðferð persónuupplýsinga, ásamt því að kynningarfulltrúi stofnunarinnar og yfirmaður lögfræðideildar voru kölluð inn síðar um daginn.

[1] Fellt brott vegna trúnaðar og á það við á sambærilegan hátt hér eftir
[2] Forrit sem opnar á aðgang að netþjónum eða kerfum fram hjá hefðbundinni aðgangsstýringu.

Kl. 13:04 var fyrsti sérfræðingurinn mættur í vaktstöð CERT-ÍS, en þeirri vakt lauk 19:35 sama dag. Áfram var unnið frá 23:45 til 0:42 við að dreifa þá nýkomnum upplýsingum. Símsambandi og tölvupóstsamskiptum var haldið við lykilaðila allan tímann.

VIÐBRÖGÐ

Strax var fylgt verkferli CERT-ÍS um [...]. Við greiningu kom í ljós að atburðarásin væri kominn út fyrir þennan feril þar sem innbrotið var yfirstaðið og hin stolnu gögn höfðu verið birt, enda um 11 tímar liðnir frá eyðileggingu vefsíðunnar. Var því farið eftir öðrum undirferli sem lýtur að [...].

Til að framkvæma öll viðbrögð á markvissari hátt, var verkum skipt milli CERT-ÍS og PFS. Til að starfsmenn CERT-ÍS gætu einbeitt sér að tæknilegum úrlausnum og samskiptum við Vodafone og aðra aðila innan þjónustuhóps síns, tók PFS að sér allt er snéri að fjölmiðlum og samskipti við aðila innan stjórnkerfisins. Fjölmiðlar voru strax byrjaðir að hafa samband við stofnunina, hver á fætur öðrum. Það sýndi sig strax þennan dag og næstu daga hversu mikilvæg og tímafrek vinna felst í samskiptum og upplýsingagjöf við fjölmiðla. Þau samskipti sneru til að byrja með að umræddu öryggisatviki. Næstu daga og vikur leituðu fjölmiðlar síðan svara hjá stofnuninni um ýmsa þætti varðandi netöryggi almennt. Ljóst er að netöryggissveitin hefði ekki haft bolmagn til að sinna slíkum samskiptum og upplýsingagjöf ásamt tæknilegri vinnu sinni.

Kl. 13.18 var rætt símleiðis við [...] Vodafone og gagna aflað um málið. Samskipti við [...] Vodafone voru stöðug yfir daginn til að fylgja eftir stöðu mála.

Kl 13.47 Hringir forstjóri PFS í [...] hjá Innanríkisráðuneytinu og ræðir um atburðinn.

Á þessum tíma fengust þær upplýsingar frá Vodafone að búið væri að virkja viðbragðsferla, viðeigandi aðilar hefðu verið kallaðir inn og vinna við málið væri í fullum gangi. Einnig kom fram að rannsókn á innbrotinu væri yfirstandandi og í það verk hefðu verið fengnir færustu sérfræðingar. Borist höfðu tæknileg gögn frá Vodafone sem innihéldu [...] og fékkst leyfi til að miðla þeim áfram, en verkferlar CERT-ÍS gera kröfu um slíkt samþykki. Á þessari stundu fékkst ekki uppgefið hjá Vodafone með óyggjandi hætti hvaða leið hefði verið farin inn í kerfi þeirra, enda getur verið margs konar óvissa í upphafi rannsóknar á slíkum málum.

Strax eftir að meðhöndlun öryggisatviksins hófst var það metið svo að viðbúnaðarstig 1 (óvissuástand)[3] ríkti í samræmi við ákvæði reglugerðar um starfsemi CERT-ÍS. Felur það í sér að sveitin geri viðeigandi aðilum þjónustuhópsins viðvart og meti hvort hefja þurfi neyðarsamráð með viðbúnaðarstigi 2. Tilkynning um slíkt er að öllu jöfnu ekki send til annarra en viðeigandi aðila þjónustuhópsins. Fyrsta stig í meðhöndluninni snýst um að afla frekari upplýsinga um atvikið til að geta metið umfang vandamálsins. Í framhaldinu hefst greiningarstarf og eru mótaðgerðir mótaðar þar á eftir. Ekki komu fram vísbendingar um að atvikið væri útbreitt eða beindist að fleiri aðilum og því var á þessum tíma ekki talin þörf á formlegu neyðarsamráði, samkvæmt ákvæðum reglugerðar 475/2013 um málefni CERT-ÍS netöryggissveitar. CERT-ÍS lýsti því ekki yfir viðbúnaðarstigi 2[4] (hættuástandi) þar sem atvikið náði ekki skilgreindum viðmiðum þess, þ.e. ástand sem hefur eða mun líklega hafa skaðleg áhrif á rekstrarhæfni ómissandi upplýsingainnviða. Í þessu samhengi er vert að benda á að ekki eru allir hlutar almennra fjarskiptaneta *ómissandi upplýsingainnviðir*[5]. Aðeins þeir hlutar sem eru nauðsynlegir til

[3] Úr reglugerð 475/2013 - „Viðbúnaðarstig 1: Óvissa vegna öryggisatviks sem gæti valdið ógn gagnvart rekstrarhæfni ómissandi upplýsingainnviða og getur hugsanlega valdið tjóni eða þjónusturofi, þótt ekki liggi fyrir endanleg þekking á skaðlegri virkni öryggisatviksins né mögulegu umfangi þess."

[4] Úr reglugerð 475/2013 - "Viðbúnaðarstig 2: Hættuástand vegna öryggisatviks sem hefur haft skaðleg áhrif á rekstrarhæfni eins eða fleiri ómissandi upplýsingainnviða eða mun að öllum líkindum hafa skaðleg áhrif á slíka innviði með ófyrirséðum afleiðingum."

[5] Úr reglugerð 475/2013 - "Ómissandi upplýsingainnviðir: Upplýsingakerfi þeirra mikilvægu samfélagslegu innviða sem tryggja eiga þjóðaröryggi, almannaheill og margs konar öflun aðfanga í þróuðu og tæknivæddu þjóðfélagi. Um er að ræða þann tækja- og hugbúnað sem nauðsynlegur er til reksturs og virkni kerfisins og þær upplýsingar sem þar eru hýstar eða um kerfið fara. Ríkislögreglustjóri skilgreinir ómissandi upplýsingainnviði."

reksturs og virkni kerfisins teljast ómissandi, en vinnu ríkislögreglustjóra við endanlega skilgreiningu þessara innviða er ekki enn lokið.

Við áframhaldandi atburðarás hélt netöryggissveitin áfram að fylgja verkferli um [...].

Kl 13.54 var [...] upplýstur um stöðuna símleiðis og í kjölfarið reynt að ná sambandi við [...] en það gekk ekki. [...] tilkynnir að fyrirtækið hafi þegar í stað virkjað öryggisáætlun sína.

Á þessum tíma var ekki staðfest af Vodafone hvaða gögnum hefði verið stolið. Því var óskað upplýsinga frá Vodafone um það.

Kl 13.55 upplýsti [...] Vodafone forstjóra PFS símleiðis um að umrædd gögn væru SMS skeyti sem send höfðu verið í gegnum vefgátt fyrirtækisins.

Kl 14:13 Aðilar innan stjórnsýslunnar óska upplýsinga um stöðu mála.

Kl. 14.15 var sett af stað vinna við að afla afrits af gögnunum sem láku, enda mikilvægt að kanna hvað þau innihéldu.

Kl. 14.25 var hafist handa við að greina innihald gagnanna og staðfest að í skránni voru SMS, notendanöfn, ókóðuð lykilorð o.fl.

Kl 14.36 náðist loks í tengilið hjá [...] og sem var upplýstur um stöðuna, en sá tengiliður sem sveitin hafði áður reynt að ná í var staddur erlendis. Á þessum tíma voru bæði [...] komin í samband við CERT-ÍS og meðvituð um málið, en sáu ekki að neitt grunsamlegt væri í gangi í eigin kerfum. Báðu þau um frekari gögn um málið, en á þeim tíma hafði CERT-ÍS einungis upplýsingar um [...], en önnur staðfest gögn voru ekki til staðar.

Kl 14.51 sendi CERT-ÍS upplýsingar um [...] til [...].

Kl. 15.11 komu [...] til fundar hjá PFS.

Kl. 15.29 var staðfest af hálfu Vodafone að stolnu SMS gögnin væru aðeins úr vefkerfi tengdu þjónustusíðum fyrir notendur, en ekki úr SMS farsímaþjónustu (SMSC) Vodafone. Þessarar staðfestingar var óskað af CERT-ÍS að beiðni forstjóra PFS sem taldi rétt að slíkar upplýsingar yrðu staðfestar formlega af Vodafone til að eyða óvissu um það hvort viðbrögð CERT-ÍS væru í réttum farvegi. Einnig var leitað eftir upplýsingum frá Vodafone um innbrotið sjálft og aðferðir sem notaðar voru við það, en málið var þá enn í rannsókn og ekki hægt að veita meiri upplýsingar.

Á þessum tíma var endurmetið hvort atvikið snerti ómissandi upplýsingainnviði. Ekki var talið svo vera þar sem umrætt vefkerfi er ekki ómissandi hluti fjarskiptakerfis Vodafone. Þó var atvikið litið alvarlegum augum vegna þess að um viðkvæm persónugreinanleg gögn væri að ræða og þess hversu margir viðskiptavinir Vodafone áttu í hlut.

Kl. 15.45 var unnið að gerð fréttatilkynningar.

Kl. 16.00 mættu til upplýsingafundar hjá PFS [...], ásamt [...] Vodafone.

Kl. 16.45 sendi CERT-ÍS gögn um [...] til [...], en fyrirspurnir höfðu borist frá þeim. Var þetta talið nauðsynlegt svo umræddir aðilar gætu gert viðeigandi verndarráðstafanir.

Kl. 16.50 voru drög að sameiginlegri fréttatilkynningu PFS og innanríkisráðuneytisins samræmd við [...] Vodafone.

Kl. 17.55 var fréttatilkynning birt á vefsíðu PFS og þar með send sjálfkrafa á póstlista vefsins, ásamt því sem hún var send sérstaklega á alla fjölmiðla með tölvupósti.

Kl. 18.10 var staðan aftur metin og ákveðið að ekki væri frekari aðgerða þörf af hendi CERT-ÍS, að svo stöddu. Á þessum tímapunkti voru öryggissérfræðingar enn að störfum hjá Vodafone við greiningu atviksins og var beðið frekari upplýsinga frá þeim.

Þann 1. desember:

Kl. 00.19 betri greining hafði farið fram innan Vodafone, sem upplýsti CERT-ÍS um [...].

Kl. 00.30 CERT-ÍS sendir frekari upplýsingar um [...] til [...].

Kl. 11.45 Forstjóri [...] hringir í forstjóra PFS og upplýsir að fyrirtækið hafi farið ítarlega yfir stöðuna, bæði hvað varðar mögulega hliðstæða atburði og einnig hvort varðveisla gagna í kerfum [...] sé í samræmi við lagafyrirmæli.

Kl. 13.38 Forstjóri PFS hringir í forstjóra [...] til að fara yfir stöðuna varðandi innbrotið hjá Vodafone og varðveislu gagna.

Næstu dagar

Næstu daga á eftir skýrðust mál töluvert og áherslur CERT-ÍS og PFS breyttust í ljósi frekari upplýsinga og framgangs málsins. Upplýsingaskipti við Vodafone og samræming aðgerða með þeim, færðist yfir í að afla réttari gagna um málsatvik, sem og að sinna samskiptum við fjölmiðla. Jafnframt þurfti að veita ráðleggingar til þeirra sem hlut áttu að máli og öðrum sem reka óskyld kerfi og voru í sambandi við sveitina með áhyggjur af eigin kerfum.

Önnur verkefni PFS í kjölfarið, voru samskipti við ráðuneyti og Alþingi, ásamt því að svara miklum fjölda fyrirspurna frá fjölmiðlum, bæði varðandi öryggisatvikið sjálft og netöryggi almennt.

CERT-ÍS sinnti einnig áframhaldandi atriðum sem komu upp og eru talin upp hér að neðan. Jafnframt varð annað, en ótengt, öryggisatvik hjá öðru fyrirtæki á mánudagskvöldinu 2. desember, þar sem menn voru meira vakandi en ella vegna undangenginna atburða.

Forstjóri og forstöðumenn tæknideildar og lögfræðideildar PFS mættu á fund umhverfis- og samgöngunefndar Alþingis þann 5. desember vegna málsins, ásamt fulltrúum Persónuverndar og RLS. Forsvarsmenn Vodafone, og síðan Símans, NOVA og Tals voru einnig boðaðir sama dag á fund nefndarinnar.

Hin stolnu gögn

Fljótlega á laugardeginum var tekin eindregin afstaða af hálfu Vodafone um að dreifing stolinna gagna væri ólögleg og alvarlegt brot á friðhelgi fólks[6]. Í kjölfarið bönnuðu fjölmörg fyrirtæki starfsfólki sínu að reyna að nálgast eða geyma gögnin á kerfum þeirra, en þetta bann náði einnig til fjölmargra öryggissérfræðinga. Innihald gagnanna var ekki aðeins viðkvæmar upplýsingar úr SMS sendingum, heldur einnig lykilorð og notendanöfn. Slíka lista notendanafna og lykilorða er hægt að nýta af öryggissérfræðingum m.a. til að vara eigin starfsmenn og viðskiptavini við, en einnig til að kanna öryggi eigin kerfa m.t.t. notenda sem hafa notað sama lykilorð á mörgum stöðum. Þessum upplýsingum hafði þá þegar verið dreift ólöglega af árásaraðilanum og þær því almennt aðgengilegar og mögulega í höndum annarra tölvuþrjóta. Hins vegar var talið að um mögulegt brot á lögum um persónuvernd væri að ræða ef CERT-ÍS færi að dreifa hluta þeirra til annarra aðila, jafnvel þó svo að það væri í þeim tilgangi að tryggja öryggi starfsmanna og viðskiptavina sinna og þannig takmarka mögulegt tjón atviksins. Olli þetta vanda hjá fjölda fyrirtækja sem óttuðust að hin stolnu gögn yrðu notuð til að fara ólöglega inn í kerfi þeirra.

Beiðnir bárust PFS og CERT-ÍS um að vera milligönguaðili með þann hluta gagnanna sem hægt væri að nota til að draga úr mögulegu tjóni. Beiðnirnar komu frá bönkum, nokkrum þjónustuveitendum og hýsingaraðilum.

[6] Sjá færslu færslu á Facebook síðu Vodafone, 30. nóvember, 2013, kl 15:45.

Vodafone var þessu samþykkt. Af fyrrgreindum ástæðum var sú ákvörðun tekin að lykilorðum án notendanafna yrði dreift af CERT-ÍS til þjónustuhópsins og bankanna, en slík einfölduð skrá hefur takmarkaðra notagildi. Einnig var Vodafone hvatt til að koma upp möguleika á að samkeyra aðrar skrár við stolnu gögnin, með undanþágu frá Persónuvernd, t.d. í samvinnu við einstök þjónustufyrirtæki á þessu sviði. Eðlilegt þótti að krafa væri um rekjanleika á verkferlum við slíka samkeyrslu hjá viðkomandi þjónustufyrirtæki í formi ISO vottunar eða sambærilegs fyrirkomulags.

Rannsókn á innbroti og dreifing slíkrar vitneskju

Fyrsta sólarhringinn eftir innbrotið, voru sem fyrr segir helstu öryggissérfræðingar landsins fengnir af Vodafone til að rannsaka innbrotið. Staðfestar upplýsingar um hvernig brotist hafði verið inn komust þó ekki í hendur CERT-ÍS fyrr en seinni hluta 2. desember, og þá aðeins í trúnaði.

Samkvæmt verklagsreglum CERT-ÍS þarf samþykki ábyrgðaraðila upplýsinganna til þess að sveitin geti dreift þeim til þjónustuhópsins. Er þetta m.a. gert til að viðhalda trúnaði milli sveitarinnar og þjónustuhóps hennar, sem er öllum netöryggissveitum mikilvægur. Ekki er fyrir hendi ótvíræð heimild í lögum um að dreifa slíkum gögnum án slíks samþykkis. CERT-ÍS upplýsti þó þjónustuhópinn óformlega um það mat sitt að kerfi annarra væru ekki í sambærilegri hættu. Byggði það mat á því að um var að ræða sérhannað kerfi sem ekki væri í notkun annars staðar. Taldi sveitin sig ekki hafa leyfi Vodafone til að miðla upplýsingum um eðli innbrotsins og kerfisins innan þjónustuhópsins fyrr en á fundi að kvöldi 4. desember og þá í mjög takmarkaðri mynd. Í ljósi þess að kerfi annarra, sem þjóna sama tilgangi, voru ekki talin í hættu og fyrri samskipta við þjónustuhópinn hvað þetta varðar var þessum upplýsingum ekki formlega miðlað strax til hans, þótt málið ætti sem slíkt erindi við þjónustuhópinn. Upplýsingar sem þessar eru mikilvægar á fyrstu stigum öryggisatvika til að finna þau kerfi sem mögulega eru veik fyrir sömu tegund árásar. Strax á laugardeginum var komin fram eindregin ósk frá þjónustuhópnum um að fá þessar upplýsingar.

Tekið skal fram að CERT netöryggissveitir eru almennt ekki í því hlutverki að rannsaka öryggisatvik með það að markmiði að upplýsa um brot eða handsama afbrotamenn. Slíkt er alla jafna á höndum lögreglunnar. Hlutverk netöryggissveitanna snýr fyrst og fremst að því að takmarka frekara tjón og eftir bestu geta að koma í veg fyrir að sömu aðferðum sé hægt að beita annars staðar.

Annar hluti: Hvað læra má af viðbrögðum CERT-ÍS og PFS

Þótt þetta mál hafi ekki snert ómissandi upplýsingainnviði Íslands, er Vodafone málið fyrsta málið af þessari stærðargráðu og af þeim toga sem kemur upp eftir að netöryggissveitin tók formlega til starfa í júní 2013. Öryggisatvikið, þ.e. innbrotið sjálft og stuldur gagnanna, var í raun þegar yfirstaðið er sveitin kom fyrst að því. CERT-ÍS, eins og aðrar netöryggissveitir, sinnir fyrst og fremst stuðningi og viðbrögðum. Þótt ekki hafi reynt mikið á tæknilega úrlausn sveitarinnar í þessu tiltekna máli, né samhæfingu atviksaðila, þar sem atvikið snerti aðeins Vodafone beint, var CERT-ÍS virkt í upplýsingamiðlun, ásamt því að PFS sinnti ákveðnu hlutverki í ráðgjöf og miðlun upplýsinga til annarra stjórnvalda.

Hér fyrir neðan eru dregin saman þau atriði málsins sem helst má draga lærdóm af, sem og þau atriði í verklagi CERT-ÍS sem sýndu gildi sitt. Aftast í kaflanum er svo listi yfir þá punkta þar sem helst þarf að gera úrbætur í ljósi þessa atburðar.

Tengiliðaskrá CERT-ÍS

Fljótlega eftir að formleg starfsemi sveitarinnar hófst, tóku starfsmenn hennar saman lista yfir, þjónustu og tengiliði helstu fyrirtækja innan fjarskiptamarkaðarins. Fór sú vinna þannig fram að sveitin óskaði eftir þessum upplýsingum frá fyrirtækjum í þjónustuhópnum. Gagnvart nokkrum þeirra þurfti að ítreka beiðni sveitarinnar um að fá umbeðnar upplýsingar og höfðu svör á þessum tíma ekki borist frá öllum. Þegar öryggisatvikið hjá Vodafone kom upp gekk vel að ná í þau fyrirtæki sem höfðu sinnt þessari skráningu vel og haldið henni uppfærðri. Tengiliðaskráin sannaði því gildi sitt með ótvíræðum hætti og sýndi fram á nauðsyn þess að samskiptaupplýsingar séu ætíð réttar og tiltækar. Um leið varð ljóst mikilvægi þess að persónuleg tengsl séu milli starfsmanna CERT-ÍS og þeirra sem eru innan þjónustuhóps sveitarinnar.

Þjálfun, samvinna og samræming aðgerða

Skömmu fyrir atvikið hafði sveitin haldið fyrstu innanlandsæfinguna með aðilum fjarskiptamarkaðarins. Jafnframt hafði sveitin, ásamt íslenskum fjarskiptafyrirtækjum, tekið þátt í sam-evrópskri netöryggisæfingu haustið 2012 (Cyber Europe 2012). Sú reynsla og þjálfun sem fékkst úr þessum æfingum nýttist vel í þessu atviki, bæði í vinnu netöryggissveitarinnar sjálfrar og ekki síður meðal þeirra fulltrúa fyrirtækjanna sem höfðu verið þátttakendur í æfingunum. Áhersla í þessum æfingum voru sviðsett öryggisatvik, meðhöndlun þeirra, samræming viðbragða og upplýsingamiðlun. Reynslan af æfingunum nýttist einnig vel til að mynda verkaskiptingu milli netöryggissveitarinnar annars vegar og annarra starfsmanna PFS hins vegar.

Viðbúnaðarstig CERT-ÍS

Viðbúnaðarstig í starfsemi CERT-ÍS eru skilgreind í reglugerð 475/2013. Þau eru númeruð 1 (óvissa), 2 (hættuástand) og 3 (neyðarástand). Við viðbúnaðarstig 2 hefst formlegt samráð þeirra aðila sem að málinu koma, og við viðbúnaðarstig 3 (neyðarástand) er RLS gert viðvart um málið sem metur í framhaldinu hvort embættið lýsi yfir almannavarnarástandi.

Í þessu tilviki miðlaði CERT-ÍS ekki til ytri aðila upplýsingum um að sett hefði verið á viðbúnaðarstig 1 (óvissustig). Skoða þarf hvort breyta þurfi verklagsreglum sveitarinnar á þann veg að viðbúnaðarstig 1 sé tilkynnt öllum tengiliðum innan þjónustuhópsins. Gildandi verklagsreglur voru samdar með það í huga að óvissustigi væri lýst nokkuð oft yfir, en nú hefur sýnt sig að slíku er ekki að dreifa.

Samkvæmt verklagsreglunum er mat viðbúnaðarstigs aðallega tengt því hvort öryggisatvikið tengist ómissandi upplýsingainnviðum, sem reyndist ekki vera í þessu tilviki. E.t.v. þarf að víkka þessa skilgreiningu út og fella undir hættustig (og e.t.v. önnur viðbúnaðarstig) atburði sem ekki tengjast ómissandi upplýsingainnviðum beint, t.d. ef öryggisatburðurinn tengist persónuupplýsingum í miklum mæli eða upplýsingarnar eru þess eðlis að geta verið viðkvæmar.

Upplýsingagjöf til stjórnvalda (ráðuneytis) - Neyðarráð

Vegna alvarleika málsins og mikillar fjölmiðlaumfjöllunar var ákveðið í samráði við innanríkisráðuneytið að [...]. Myndaðist því nokkurs konar óformlegt neyðarráð innan veggja PFS með aðkomu þessara aðila. Neyðarráð sem hafa yfirsýn yfir víðara svið en þau fyrirtæki eða aðilar sem eiga í vanda og koma saman við stóráföll eru þekkt erlendis. Hugmyndir hafa verið uppi hérlendis um slíkt fyrirfram ákveðið skipulag sem gæti sinnt ákvarðanatöku á hærra stigi. Æskilegt er að slíku skipulagi væri formlega komið á hérlendis.

Skráning upplýsinga

Upplýsingakerfi CERT-ÍS fela meðal annars í sér sérhæft mála- og atvikaskráningarkerfi fyrir netöryggissveitir. Eingöngu starfsmenn CERT-ÍS hafa aðgang að þessu málaskráakerfi og ekki aðrir starfsmenn stofnunarinnar. Er það gert af ásettu ráði til að tryggja aðskilnað milli sveitarinnar og eftirlitshlutverks PFS með það að markmiði að viðhalda trúnaði við þjónustuhópinn. Einnig eru rekin aðgreind tölvupóstkerfi. Þessi markvissi aðskilnaður kerfanna gerir það að verkum að aðrir starfsmenn PFS hafa ekki aðgang að kerfum netöryggissveitarinnar. Þar sem þetta mál var ekki eingöngu til meðhöndlunar af CERT-ÍS, heldur komu nokkrir aðrir starfsmenn stofnunarinnar að málinu, er viss hluti af upplýsingum þessa máls skráður innan kerfa PFS, (stjórnsýsluhluta) svo sem tölvupóstar til og frá starfsmönnum stofnunarinnar og samskipti við þá er koma vilja að stjórnsýslukærum vegna atviksins. Til að tryggja enn frekar aðskilnað í rekstri CERT-ÍS og og annarrar starfsemi PFS er yfirflutningur á gögnum milli þessara kerfa ekki leyfður. Meta þarf hvort þörf sé á að endurskoða þessar verklagsreglur. Í viðbrögðum við öryggisatvikum er mikilvægt að heildarmynd af stöðunni sé sem skýrust á hverjum tíma og henni sé jafnóðum miðlað til þeirra sem sinna meðhöndlun málsins. Í því ljósi er grundvallaratriði að skráðar séu t.d. tímasettar færslur um hvað er að gerast á hverjum tíma og hvað hver og einn gerir. Atvikaskráningarkerfið sem sveitin notar er sem slíkt tímasett dagbók, en vegna takmarkaðs aðgengis annarra starfsmanna að því kerfi reyndist notkun venjulegra stílabóka hentugri í sumum tilfellum. Í þeim tilgangi að móta og uppfæra jafnóðum heildarstöðumynd og til að auðvelda greiningu viðbragða eftir á, væri æskilegt að vinna þetta alfarið rafrænt.

Fjölmiðlastefna

Þetta netöryggisatvik varð mjög fljótt á vitorði almennings vegna þess að gerandinn eyðilagði vefsíðu Vodafone, skrifaði um það á Twitter og dreifði stolnum gögnum opinberlega. Því voru alls kyns upplýsingar um málið komnar fram í fjölmiðlum og netheimum strax um hádegið og var þar um að ræða allt í senn réttar, ónákvæmar og rangar upplýsingar um málsatvik. Fljótlega eftir að aðgerðir voru hafnar af hálfu CERT-ÍS kom í ljós nauðsyn þess að koma réttum upplýsingum til þeirra borgara sem orðið höfðu fyrir skakkaföllum af þessari árás. Þegar þær upplýsingar höfðu fengist með fundi PFS/CERT-ÍS, forsvarsmanna Vodafone, [...] í húsnæði PFS var ráðist í gerð sameiginlegrar fréttatilkynningar til fjölmiðla til að reyna að rétta upplýsingaflæðið af. Sú vinna tafðist, m.a. vegna skorts á fyrirfram ákveðnu skipulagi innan hópsins við að taka sameiginlega á málum eins og þessu. Hér kom í ljós að formlega skipað neyðarráð hefði líklega verið betur til þess fallið að fjalla um þetta mál. Þegar þessari vinnu loks lauk var ekki tekið mið af fréttatilkynningunni í umfjöllun fjölmiðla í útvarpi og sjónvarpi í kvöldfréttum.

Tilkynning og viðbragðstími

Frá því að atvikið uppgötvaðist innan Vodafone og þar til viðbragð CERT-ÍS hófst liðu um 11 klukkutímar. Má rekja þetta til þeirra aðferða sem voru notaðar til að tilkynna um atvikið til sveitarinnar, en þær ætti að skoða í ljósi fyrirliggjandi upplýsinga á hverjum tíma. Þegar upphaflega tölvupósttilkynningin er send til CERT-ÍS kl. 08:27 var mönnum ekki ljóst að um gagnaleka væri að ræða. Það var hins vegar ljóst þegar haft var samband símleiðis kl. 12:19. Telja verður æskilegt að minnka þann tíma sem líður frá uppgötvun atviks þar til sveitin er að fullu meðvituð um málið. Því ætti að huga að fyrirkomulagi starfstíma sveitarinnar sem og aðferðum við tilkynningar til hennar.

Eiginlegur viðbragðstími sveitarinnar í þessu tilviki voru um 45 mínútur, eða frá því að símhringing barst frá Vodafone og þar til fyrsti starfsmaður var mættur í starfsaðstöðu CERT-ÍS.

TÆKNILEG VIÐBRÖGÐ OG MÖNNUN

Meðhöndlun netöryggisatvika samanstendur af tæknilegri greiningu, tæknilegum aðgerðum og upplýsingamiðlun til þeirra netveitna og annarra rekstraraðila sem í hlut eiga. Ábyrgð og framkvæmd tæknilegra aðgerða er ávallt í höndum rekstraraðila hvers kerfis á meðan CERT-ÍS sinnir m.a. upplýsingamiðlun milli aðila. Vegna umfangs þessa máls dreifðist heildar greiningarvinnan á nokkra aðila, svo sem sérfræðinga sem Vodafone fékk sér til aðstoðar, starfsmenn Vodafone og CERT-ÍS. Vegna þess hve CERT-ÍS hefur fáa starfsmenn, hefur verið lögð höfuðáhersla á að starfsmenn hennar hafi frekar þjálfun á mörgum sviðum, í stað þess að sérhæfa sig á vissum tæknilegum sviðum eins og meðhöndlun sérhæfðra öryggisatvika, tölvurannsóknir o.fl. Miklar væntingar eru til sveitarinnar, en ljóst er að geta hennar til að meðhöndla öryggisatvik er háð þeim mannafla sem þarf í slík verk. Strax við fyrstu upplýsingar sem sveitin fékk frá Vodafone var ljóst að færustu sérfræðingar í netöryggi væru mættir þeim til aðstoðar. Má huga að því hvort starfsmenn CERT-ÍS hefðu átt að koma þar að, en ljóst er að hjá sveitinni var ekki til staðar sá mannskapur né sérhæfð kerfisþekking á þessu tiltekna tækniumhverfi Vodafone sem hefði þurft til að fara og aðstoða Vodafone beint. Af þessum sökum náði tæknileg greiningarvinna CERT-ÍS aðeins til þess að greina hin stolnu gögn og meta þær upplýsingar sem bárust frá Vodafone. Var starfsfólk CERT-ÍS sömuleiðis upptekið við upplýsingamiðlun milli fyrirtækja, sem er eitt kjarnahlutverka sveitarinnar.

Jafnframt má leiða að því líkur að reynsla sveitarinnar og PFS hafi ekki nýst að fullu þar sem hópstjóri CERT-ÍS, var erlendis, þegar öryggisatvikið varð. Hið sama gildir um forstöðumann tæknideildar sem var staddur í helgarfríi úti á landi. Þessir aðilar voru þó í stöðugu símsambandi, en líkast til hefði verið enn meiri slagkraftur við úrlausn málsins með því að kalla þessa starfsmenn strax á vettvang.

RÁÐLEGGINGAR UM ÚRBÆTUR HJÁ CERT-ÍS

- Mikilvægt er að CERT-ÍS sé nægilega mannað [...]
- [...]
- [...]
- [...]
- [...]
- [...]
- [...]
- Meta hvort endurskoða þurfi viðmið um viðbúnaðarstig CERT-ÍS, svo sem hvort öryggisatvik hafi stjórnmálalegan vinkil, snerti persónuupplýsingar og/eða rati í mikla opinbera umfjöllun, o.s.frv.
- Mikilvægt er að endurskoða tilkynningu um og afléttingu viðbúnaðarstiga.
- Efla þarf fyrirkomulag netöryggissveitarinnar til að móttaka, greina, vinna úr, dreifa tilkynningum um öryggisatvik, sem og getu fjarskiptafyrirtækjanna til að bregðast við í samræmi.
- Bæta þarf enn frekar skráningu tengiliða þeirra fyrirtækja sem ekki hafa sinnt boði þar um.
- Koma þarf upp virkum samráðsvettvangi innan þjónustuhópsins um netöryggi.
- Efla þarf getu sveitarinnar til að eiga samskipti við notendahópinn á mismunandi stjórnunarstigum fyrirtækjanna (þ.e. tæknimenn/stjórnendur)
- Æskilegt væri að formgera skipulag neyðarráðs á efri stigum stjórnkerfis og skilgreina hverjir skuli skipa það.
- Mikilvægt er að beina upplýsingamiðlun til pólitískt kjörinna fulltrúa með formlegum hætti, t.d. innan neyðarráðsins.
- Endurskoða þarf upplýsingamiðlun til almennings þegar öryggisatvik verður og leggja áherslu á aukna getu til virkra og ábyrgra almannatengsla þegar áföll dynja yfir.

RÁÐLEGGINGAR UM ÚRBÆTUR Í LAGAUMHVERFI CERT-ÍS

- Færa þarf CERT-ÍS bráðabirgðaheimildir til að miðla hratt gögnum sem snerta öryggisatvik til þjónustuhópsins og annarra aðila, sem hægt verði að grípa til þegar viðbúnaðarstigi hefur verið lýst yfir. Slík gögn geta innihaldið viðkvæmar upplýsingar, t.d. persónugreinanleg gögn og gögn um innri kerfi aðila.