Belgisch Instituut voor
postdiensten en telecommunicatie

Eindverslag van de Raad van het BIPT van 14 september 2020 betreffende het incident bij Proximus op 5 april 2019

NIET-VERTROUWELIJKE VERSIE

Belgisch Instituut voor postdiensten en telecommunicatie
Ellipsgebouw C | Koning Albert II-laan 35 | 1030 Brussel
T +32 2 226 88 88 | **F** +32 2 226 88 77 | **www.bipt.be**

INHOUDSOPGAVE

Executive summary

1. Op 5 april vond een technisch incident plaats bij Proximus waardoor een zeer groot deel van spraakoproepen van en naar Proximus niet meer kon plaatsvinden.

2. De oorzaak van het incident was een technische softwarefout die door een combinatie van omstandigheden een essentiële netwerkcomponent deed falen.

3. Proximus nam de dag zelf enkele voorlopige technische maatregelen om de softwarefout niet meer te laten optreden. In de weken nadien werd een permanente oplossing geïmplementeerd.

1. Inleiding

4. Dit verslag is een analyse van het incident van 5 april 2019 op het Proximus-netwerk. Door het falen van een essentieel netwerkelement was communicatie tussen het vaste Proximus-netwerk en andere netwerken tijdelijk onmogelijk. Als gevolg hiervan waren gedurende het incident ook de nooddiensten slechts beperkt beschikbaar.

5. Deze analyse omvat zowel het juridische kader, de afhandeling tijdens het incident als de onderliggende technische oorzaak. In de periode na het incident werden reeds verschillende stappen gezet om een herhaling van gelijkaardige gebeurtenissen te voorkomen. Ook deze worden in dit verslag beschreven. Tot slot bevat dit verslag enkele voorstellen tot aanbevelingen en de reactie van Proximus hierop.

2. Juridisch kader

6. In het kader van de wet van 13 juni 2005 betreffende elektronische communicatie (hierna WEC) kan het BIPT controleren of Proximus (preventieve) maatregelen treft om een ononderbroken toegang tot de nooddiensten te garanderen (artikel 107).

7. Het BIPT kan controleren of Proximus (preventieve) maatregelen treft om de risico's voor de veiligheid van hun netwerken of diensten goed te beheersen en om de impact van veiligheidsincidenten op gebruikers en onderling verbonden netwerken zo laag mogelijk te houden (artikel 114, § 1, van de WEC) en kan hiervoor bindende instructies geven (artikel 114/2 van de WEC).

8. In het kader van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en in de hoedanigheid van inspectiedienst voor de sector van elektronische communicatie, kan het BIPT controleren of het beveiligingsplan van de exploitant (B.P.E.) (in dit geval Proximus) wel degelijk de maatregelen bevat om het risico dat zich tijdens het incident op 5 april 2019 heeft voorgedaan, te voorkomen, te beperken en te neutraliseren (artikel 13, § 1) en of Proximus zijn B.P.E bijwerkt wanneer nodig (artikel 13, § 6).

3. Historiek

3.1. Gebeurtenissen op 5 april 2019

9. Op vrijdag 5 april 2019 om 15u30 werd het vaste netwerk van Proximus geïsoleerd door een technisch probleem in een essentiële component voor het inter-netwerkverkeer. Als gevolg hiervan was er geen communicatie tussen het vaste netwerk van Proximus en het mobiele netwerk van Proximus. Ook communicatie tussen het vaste netwerk van Proximus en de netwerken, zowel de vaste als de mobiele, van andere operatoren was niet langer mogelijk. Een bijkomend effect van dit technisch probleem was een zeer beperkte telefonische bereikbaarheid van nooddiensten. Enkel toestellen aangesloten op het vaste netwerk van Proximus konden de nooddiensten nog telefonisch bereiken. Onderstaande tabel van Proximus geeft de impact op de telefoniediensten grafisch weer. De impact van het probleem was beperkt tot telefonie. SMS en internettoegang, zowel vast als mobiel, waren niet getroffen. De nooddiensten bleven voor gebruikers van mobiele toestellen dan ook bereikbaar per SMS via het nummer 8112, het noodnummer dat in normale omstandigheden uitsluitend gebruikt wordt door doven en slechthorenden.

	TO							
FROM	100-101-112	PXS Fix	Scarlet Fix	PXS ISDN	PXS Mob	OLO	MOLO	BICS
PXS Fix	OK	OK	OK	NOK	NOK	NOK	NOK	NOK
Scarlet Fix	OK	OK	OK	NOK	NOK	NOK	NOK	NOK
PXS ISDN	NOK	NOK	NOK	NOK	NOK	NOK	NOK	NOK
PXS Mob	NOK	NOK	NOK	NOK	OK	OK	OK	OK
OLO	NOK	NOK	NOK	NOK	OK	OK	OK	OK
MOLO	NOK	NOK	NOK	NOK	OK	OK	OK	OK
BICS	NOK	NOK	NOK	NOK	Ok	OK	OK	OK

10. Om 16u05 bracht Proximus de permanentie van het BIPT op de hoogte van de situatie. De permanentie bracht vervolgens het crisiscentrum op de hoogte. Het crisiscentrum was inmiddels al door de noodcentrales geïnformeerd over de aanwezigheid van de problemen. De personeelsleden van de dienst NetSec die dat moment nog aanwezig waren in de lokalen van het BIPT hebben de permanentie geholpen met de coördinatie van de communicatie tussen het crisiscentrum, Proximus, Telenet, Orange en Voo. Gezien de aard en impact van het incident waren indirect namelijk ook klanten van de andere operatoren getroffen.

11. Om 17u51 waren de problemen bij Proximus nog steeds aan de gang en kon er nog geen uitspraak gedaan worden over een eventuele oplossing en de tijdspanne waarin deze gerealiseerd kon worden. Het crisiscentrum nodigde daarom de betrokken overheidsdiensten uit voor een crisisvergadering om 18u45. Het BIPT stuurde hierop een verbindingsofficier naar het crisiscentrum en stuurde tevens een vertegenwoordiger van het BIPT naar Proximus om de situatie van nabij te kunnen opvolgen.

12. Om 18u15 was het probleem voor nooddiensten opgelost. Dit kon echter op dat moment niet bevestigd worden en dit tijdstip werd pas na het incident bevestigd.

13. Omstreeks 18u45 meldt het crisiscentrum dat enkele noodcentrales doorgeven dat de problemen opgelost lijken. Dit kan op dat moment niet door Proximus bevestigd worden.

14. Om 18u50 was het probleem grotendeels opgelost voor alle type oproepen. Dit kon echter op dat moment niet bevestigd worden en dit tijdstip werd pas na het incident bevestigd.

15. Om 18u51 hebben alle noodcentrales bevestigd dat de telefonische toegang tot het noodnummer 112 correct lijkt te functioneren. Dit kan echter opnieuw niet bevestigd worden Proximus.

16. Om 19u start het crisiscentrum de federale fase.

17. Om 19u start bij Proximus een nieuwe vergadering van de crisiscel, bijgewoond door de vertegenwoordiger van het BIPT. Tijdens deze vergadering wordt bevestigd dat de situatie inderdaad verbetert en dat de capaciteit systematisch verhoogt. Aangezien noodoproepen prioriteit krijgen op het netwerk van Proximus, waren de noodcentrales inderdaad de eersten die merkten dat de situatie verbeterde.

18. Om 19u54 signaleren de noodcentrales van Antwerpen en Oost-Vlaanderen opnieuw problemen.

19. Om 20u14 bevestigt Proximus het bestaan van enkele *residuele* problemen, als gevolg van de gebeurtenissen eerder die dag. Hierdoor zijn nog niet alle interconnecties met de verschillende operatoren op volle capaciteit waardoor er nog steeds oproepen kunnen falen. Deze problemen zullen progressief opgelost worden in het komende uur.

20. Om 20u22 beëindigt het crisiscentrum de federale fase.

21. Om 21u25 bevestigt Proximus dat alle residuele problemen opgelost zijn. De toestand is volledig terug normaal.

3.2. Gebeurtenissen na 5 april 2019

22. Gedurende het weekend van 6 en 7 april heeft Proximus zijn netwerk extra in het oog gehouden. Er werden geen problemen meer gedetecteerd.

23. Op dinsdag 9 april bezorgde Proximus het BIPT een beperkt rapport over de gebeurtenissen van 5 april. Hierin gaf Proximus een overzicht van de tijdelijke maatregelen die het op 5 april genomen heeft om de situatie naar normale toestand te herstellen. Tevens gaf Proximus aan dat Nokia, de leverancier van de netwerkcomponent die gefaald heeft, een permanente oplossing ontwikkelt. Deze oplossing zou tijdens de nachten van 17 en 18 april geïnstalleerd worden.

24. Op vrijdag 12 april 2019 vond op het BIPT een bijeenkomst plaats om de oorzaak van de problemen van 5 april te bespreken. Deze bijeenkomst werd bijgewoond door vertegenwoordigers van Proximus, het BIPT, de FOD Economie, de FOD Volksgezondheid, de Directie 112 en ASTRID. Tijdens deze vergadering gaf Proximus meer uitleg over de oorzaak van het incident. Het betrof een software-bug die zich door een combinatie van factoren manifesteerde. Aangezien de omstandigheden op de verschillende redundante systemen identiek waren, deed deze bug de verschillende systemen gelijktijdig falen waardoor er geen redundantie meer was.

25. Op 24 april 2019 verhoorde de Raad van het BIPT Proximus over de gebeurtenissen op 5 april. [Vertrouwelijk]

26. Op 6 mei 2019 vond op het BIPT een bijeenkomst plaats om potentiële verbeteringen naar de toekomst toe te bespreken. Deze bijeenkomst werd bijgewoond door vertegenwoordigers van Proximus, het BIPT, de FOD Economie, de FOD Volksgezondheid, de Directie 112, het crisiscentrum en ASTRID. Proximus stelde er enkele technische oplossingen voor om een herhaling van een gelijkaardig incident in de toekomst te vermijden. De verschillende partijen zouden de impact van deze oplossingen tegen 7 juni 2019 onderzoeken en meedelen aan het BIPT. Het BIPT zou de andere operatoren contacteren voor hun mening over de voorgestelde oplossingen.

27. Op 17 mei 2019 vond op het BIPT een vergadering plaats tussen dezelfde partijen als op 6 mei. De scope van deze vergadering was het opstellen van een verbeterd communicatieplan in geval van incidenten met impact op de nooddiensten.

28. Op 14 juni vond op het BIPT een opvolgingsvergadering plaats om de potentiële technische oplossingen in meer detail te bespreken. ASTRID presenteerde hun reflecties bij de verschillende oplossingen van Proximus. Het BIPT stelde de input van Orange en Telenet voor. Op basis hiervan werd een beperkte lijst van oplossingen weerhouden die in meer detail uitgewerkt zullen worden tegen 12 september.

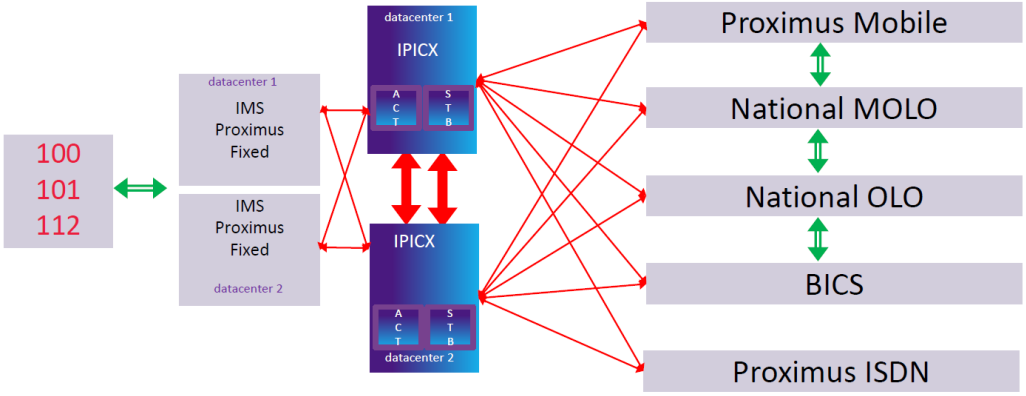
29. Op 22 juli 2019 stuurde het BIPT een eerste versie van deze analyse naar Proximus voor commentaar.

30. Op 30 september 2019 antwoordde Proximus op deze analyse.

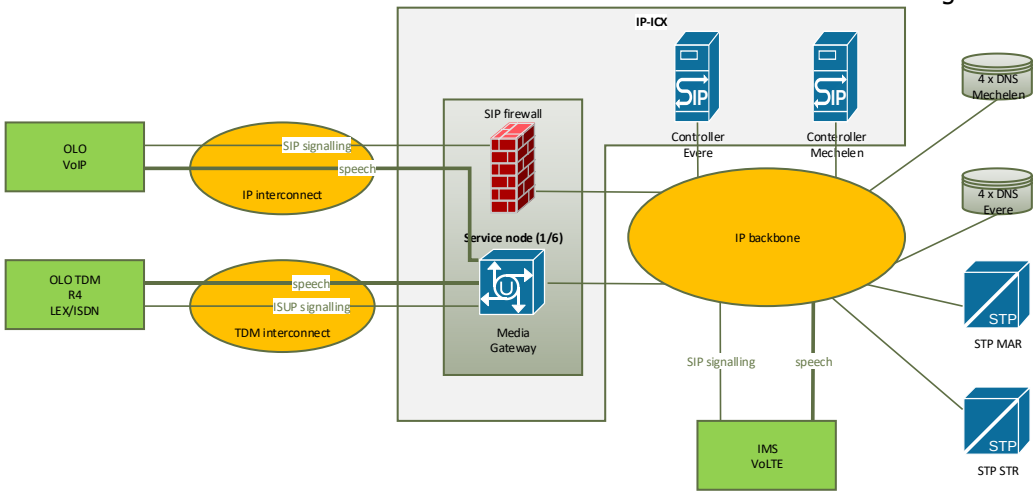
4. Technische analyse

4.1. Oorzaak

31. De root cause van het incident op 5 april was een software fout in het IPICX-platform van Proximus. Dit is het platform dat de verschillende telefonienetwerken van Proximus in verbinding stelt met de netwerken van andere operatoren. Indien dit platform slecht functioneert, heeft dit dus impact op telefoongesprekken van en naar Proximus-netwerken. In onderstaande afbeelding wordt schematisch de positie weergegeven van het IPIXC-platform van Proximus ten opzichte van de verschillende netwerken die ermee verbonden zijn. Het vaste telefonie netwerk van Proximus bevindt zich aan de linkerkant van de figuur. Alle andere netwerken die met het platform verbonden zijn, bevinden zich aan de rechterkant.



32. Het IPICX-platform is opgebouwd uit meerdere componenten, zoals weergegeven in onderstaande figuur. De oorzaak van het incident van 5 april lag in de media gateway controllers, die verantwoordelijk zijn voor het transport van spraakoproepen tussen de verschillende netwerken en de ISUP-signalisatie.



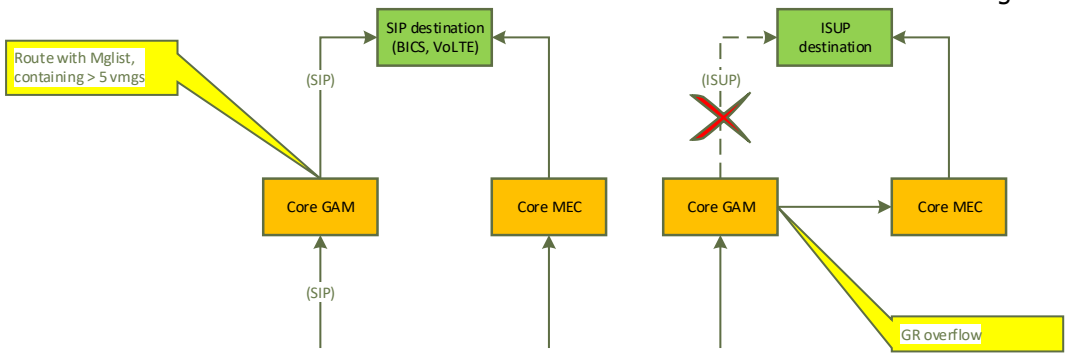
33. De media gateway controllers bevatten een softwarefout die onder specifieke omstandigheden een heropstart veroorzaakte. Tijdens een herstart is de gateway tijdelijk niet beschikbaar. In normale omstandigheden vormt dit geen probleem. Er is immers voldoende redundantie voorzien, zowel lokaal als geografisch. Aangezien de

omstandigheden op 5 april voor alle media gateway controllers identiek waren, herstartten deze allen gelijktijdig en voortdurend. Bijgevolg waren de media gateway controllers, en daardoor ook het gehele IPICX-platform niet functioneel gedurende het incident.

34. De softwarefout deed zich voor door een combinatie van 3 omstandigheden.

35. Een eerste voorwaarde voor het manifesteren van de softwarefout is de aanwezigheid van spraakverkeer over IP (in plaats van uitsluitend TDM). Dit was op 5 april het geval voor de interconnecties met BICS en Nethys. Proximus had enkele weken voordien spraakverkeer via IP geactiveerd als onderdeel van hun lange-termijn migratie van TDM naar IP. Deze verandering in het netwerk was dus indirect één van de oorzaken van het incident.

36. Een tweede voorwaarde is de aanwezigheid van *intercore-verkeer* tussen de verschillende media gateway controllers van het IPICX-platform. Intercore-verkeer is signalisatieverkeer dat zich voordoet tussen de verschillende media gateway controllers wanneer het afleveren van een oproep aan een geïnterconnecteerde partner niet lukt via één van de gateways. In dat geval zal Proximus de oproep doorsturen naar een andere media gateway controller in een ander datacenter die ook verbonden is met dezelfde geïnterconnecteerde partner. Er passeert met andere worden niet enkel verkeer *over* de media gateway controllers, maar ook *tussen* de media gateway controllers in de verschillende datacenters. Een illustratie van deze situatie staat in onderstaande figuur.



37. Op 5 april rond 15u25 kreeg de Franse operator OVH problemen met één van hun netwerkcomponenten. Als gevolg hiervan vielen de interconnecties tussen Proximus en OVH uit. Oproepen die via het IPICX-platform van Proximus passeerden en bestemd waren voor OVH, genereerden dus intercore-verkeer. OVH had immers een redundante connectie met het IPICX-platform. Er werd dus eerst geprobeerd om een oproep via één interconnectie aan OVH af te leveren. Dit mislukte door de problemen bij OVH. Vervolgens werd de oproep (als intercore-verkeer) doorgestuurd naar een andere media gateway controller om daar ook een aflevering aan OVH te proberen, wat uiteraard ook mislukte.

38. De problemen bij de Franse operator OVH waren dus de veroorzakende factor voor het incident van 5 april. Ze waren echter niet de enige factor.

39. Een derde voorwaarde voor het voordoen van de softwarefout was *memory corruption*. Door foutief geheugenbeheer in de media-gateways werd in specifieke omstandigheden, veroorzaakt door de vorige twee voorwaarden, een ongeldige lees- of schrijfoperatie uitgevoerd in het geheugen. Dit resulteerde in de crash van één van de essentiële processen op de media gateway controller met een herstart tot gevolg.

40. Bovenstaande drie voorwaarden waren alle drie noodzakelijk voor het voordoen van de fout. De eerste twee voorwaarden, namelijk de aanwezigheid van IP-verkeer en intercore-verkeer, zijn geen slechte indicatoren. Dit soort verkeer is normaal en zou geen problemen mogen veroorzaken. In combinatie met de derde voorwaarde veroorzaakten zij wel herstarts van het systeem met het niet-functioneren van het IPICX-platform tot gevolg.

41. Er dient opgemerkt te worden dat tijdens de dagen voorafgaand aan 5 april reeds enkele occasionele herstarts van de media gateway controllers werden waargenomen. Hiervoor werd reeds een 'critical' ticket geopend door Proximus bij Nokia.

42. De residuele problemen waarvan spraken naar het einde van het incident toe werden veroorzaakt door de vele herstarts. Aangezien deze herstarts veelvuldig en plots (i.e. niet op een correcte technische manier) gebeurden, waren enkele trunks in een ongeldige toestand beland waardoor er hierover geen verkeer mogelijk was.

4.2. Tijdelijke oplossing op 5 april

43. Op 5 april herstelde Proximus het IPICX-platform door twee van de voorwaarden voor de softwarefout weg te nemen.

44. De recente activering van het toelaten van IP-verkeer werd teruggedraaid. Dit nam de eerste voorwaarde voor het voordoen van de softwarefout weg. Er was immers enkel nog TDM-verkeer mogelijk.

45. Een tweede actie ondernomen door Proximus was het deactiveren van het intercore-verkeer, hetgeen de tweede voorwaarde voor de softwarefout wegnam.

46. Aan de derde voorwaarde, de memory corruption, kon Proximus zelf geen wijzigingen aanbrengen. Dit was immers een fout in de media gateway controller en niet in de netwerkarchitectuur van Proximus.

47. Beide genomen maatregelen waren zeer tijdelijk van aard. Immers, in normale toestand zouden deze soorten verkeer mogelijk moeten zijn.

48. De residuele problemen werden opgelost door de trunks manueel op een correcte manier te herstarten zodat deze in een geldige toestand kwamen en telefonieverkeer konden transporteren.

4.3. Voorlopige oplossing op 17 en 18 april

49. Na het incident van 5 april is Nokia onmiddellijk gestart met het ontwikkelen van een patch voor de oorzaak van het incident. Deze patch werd op 9 april in de testomgeving van Proximus getest met een succesvol resultaat.

50. In de nachten van 17 en 18 april werd deze patch geïnstalleerd op de operationele systemen van Proximus.

4.4. Definitieve oplossing

51. De patch werd ook geïntegreerd in de volgende release van de software voor de media gateway controllers. Dit voorkomt dat hetzelfde probleem zich herhaalt na de eerstvolgende upgrade.

5. Voorlopige aanbevelingen aan Proximus (juli 2019)

5.1. Aanbevelingen van het BIPT aan Proximus

52. Iedere aanpassing van het netwerk moet grondig getest worden alvorens deze in de productie-omgeving door te voeren. Het volstaat niet de aanpassing in isolatie te testen. Een aanpassing kan immers ook neveneffecten hebben op andere delen van het netwerk. Iedere aanpassing moet daarom in de mate van het mogelijke end-to-end getest worden in een omgeving die de omstandigheden van de productie-omgeving zo goed mogelijk benadert. Bij deze testen moet niet enkel rekening gehouden worden met de omstandigheden in het eigen netwerk, maar ook met andere omstandigheden (waaronder het uitvallen of abnormaal gedrag van interconnectie-partners).

53. Het is essentieel om ook op regelmatige basis de back-up-systemen te testen. Veranderingen aan het netwerk kunnen immers ook veranderingen aan back-up-systemen vereisen. Om te vermijden dat deze wijzigingen over het hoofd gezien worden is het aangeraden om geregeld een simulatie uit te voeren van het falen van één of meerdere componenten van het netwerk. Dit laat toe om te evalueren of de back-up-systemen in staat zijn om een panne op te vangen. Een noodscenario waar de back-up-systemen falen omdat ze niet meer actueel zijn, dient absoluut vermeden te worden.

54. Het aantal single-points-of-failure (SPOF) in een netwerk moet zoveel mogelijk gereduceerd worden. Om het risico op gelijktijdig falen van componenten met een eenzelfde functie te beperken, is het ten zeerste aangeraden om diversificatie toe te passen op deze componenten. Het gebruik van componenten van verschillende leveranciers voor eenzelfde functie verlaagt de kans dat identieke omstandigheden leiden tot het falen van verschillende systemen.

55. Indien het niet mogelijk is een SPOF weg te werken dan is het nodig hiervoor een business continuity plan (BCP) op te stellen, zodat in geval van falen onmiddellijk de nodige maatregelen genomen kunnen worden om het netwerk verder te laten functioneren, zij het dan in een gedegradeerde toestand.

56. Voor iedere upgrade of migratie op het netwerk moet een gedetailleerde planning gemaakt worden. Deze planning moet wanneer relevant ook gedeeld worden met de leveranciers van hard- of software. Indien een upgrade potentieel een grote impact heeft op het functioneren van het netwerk, dan dienen ook de nodige afspraken gemaakt te worden met deze leveranciers zodat deze in geval van nood snel kunnen bijspringen.

57. Een essentieel onderdeel van bovenvermelde planning is het fallback-plan voor het geval dat de upgrade of migratie misloopt. Dit fallback-plan moet duidelijke en precieze instructies bevatten in verband met het ongedaan maken van bepaalde wijzigingen. Indien in de loop van een upgrade of migratie problemen optreden, dan kunnen onmiddellijk de nodige acties ondernomen worden om de situatie te herstellen.

5.2. Reactie van Proximus op de aanbevelingen

5.2.1. Testen van aanpassingen aan het netwerk

58. Proximus stelt dat het aanpassingen zeer uitgebreid test en geeft meer toelichting over hoe zij te werk gaan bij de testen en het opstellen van het testplan. Proximus stelt ook dat het onmogelijk is om alle mogelijke scenario's te testen, maar dat zij hun testplan aanpassen op basis van nieuwe incidenten die zij tegenkomen.

59. Proximus heeft gelijk dat het onmogelijk is om alle scenario's te testen. Het aantal parameters van hard- en software is tegenwoordig veel te groot om alle combinaties in een realistisch tijdsvenster te testen. De situatie die zich voordeed op 5 april 2019 was een bug die zich in zeer specifieke omstandigheden voordeed waarvan het geloofwaardig is om aan te nemen dat deze niet in een standaard testplan wordt opgenomen.

5.2.2. Testen van de back-up-systemen

60. Proximus stelt dat het aanpassingen zeer uitgebreid test en geeft meer toelichting over hoe zij te werk gaan bij de testen en het opstellen van het testplan. Proximus stelt ook dat het onmogelijk is om alle mogelijke scenario's te testen, maar dat zij hun testplan aanpassen op basis van nieuwe incidenten die zij tegenkomen.

61. Proximus heeft gelijk dat het onmogelijk is om alle scenario's te testen. Het aantal parameters van hard- en software is tegenwoordig veel te groot om alle combinaties in een realistisch tijdsvenster te testen. De situatie die zich voordeed op 5 april 2019 was een bug die zich in zeer specifieke omstandigheden voordeed waarvan het geloofwaardig is om aan te nemen dat deze niet in een standaard testplan wordt opgenomen.

5.2.3. SPOFs, diversificatie en BCP

62. Proximus stelt dat het aanpassingen zeer uitgebreid test en geeft meer toelichting over hoe zij te werk gaan bij de testen en het opstellen van het testplan. Proximus stelt ook dat het onmogelijk is om alle mogelijke scenario's te testen, maar dat zij hun testplan aanpassen op basis van nieuwe incidenten die zij tegenkomen.

63. Proximus heeft gelijk dat het onmogelijk is om alle scenario's te testen. Het aantal parameters van hard- en software is tegenwoordig veel te groot om alle combinaties in een realistisch tijdsvenster te testen. De situatie die zich voordeed op 5 april 2019 was een bug die zich in zeer specifieke omstandigheden voordeed waarvan het geloofwaardig is om aan te nemen dat deze niet in een standaard testplan wordt opgenomen.

64. Proximus geeft in hun antwoord meer uitleg over de verschillende vormen en aspecten van hun BCPs. Het legt ook uit waar op dit moment de SPOF zitten, i.e. op lokaal (gemeentelijk) niveau. Proximus benadrukt ook de noodzaak om te beschikken over goede expertise bij het eigen personeel om in geval nood problemen te kunnen oplossen.

65. SPOFs op lokaal niveau zijn moeilijk uit te sluiten, maar op centraal niveau in de kritieke infrastructuur kan dit wel. Dit moet dan ook gebeuren en waar het echt niet anders kan, dienen de maatregelen genomen te worden om een uitval van een SPOF snel en effectief op te vangen.

66. Deze noodzaak aan in-house expertise is inderdaad zeer belangrijk.

5.2.4. Migratieplanning

67. Proximus licht kort toe hoe ze migraties aanpakken en wat de betrokkenheid van de leverancier is. Proximus vermeldt het change-managementproces dat ze hanteren en de fallback-voorziening hierin. Ze benadrukken tevens dat het incident van 5 april niet acuut veroorzaakt werd door een migratie, maar als gevolg van een migratiestap enkele weken voordien. Eens de oorzaak duidelijk was werd er probleemloos teruggeschakeld naar de oude configuratie.

68. Deze uitleg stemt overeen met de andere informatie die wij van Proximus ontvingen in de context van dit dossier en andere.

6. Definitieve aanbevelingen (juli 2020)

6.1. Aanbevelingen op korte termijn

69. Op basis van de voorgaande elementen uit dit rapport formuleert het BIPT enkele aanbevelingen aan Proximus.

70. Voor de implementatie van deze maatregelen beveelt het BIPT aan om gebruikt te maken van internationale erkende standaard, zoals bv. de normen uit de ISO27000-familie.

71. Het BIPT zal in het najaar van 2020 controleren of deze aanbevelingen worden opgevolgd. Het BIPT kan in een later stadium al dan niet een beslissing nemen in de vorm van bindende instructies conform artikel 114 en 114/2 van de WEC.

6.1.1. Analyse van SPOFs en bijhorende BCPs

72. Proximus dient een degelijke analyse te maken van de SPOFs in hun kritieke infrastructuur en kritieke netwerkfuncties. Deze analyse moet zowel op fysisch (hardware) als op logisch (software) niveau gebeuren. Voor elke SPOFs dient een BCP opgesteld te worden om de impact in geval van falen zo veel en zo snel mogelijk te beperken. Indien er externe expertise nodig is om een SPOF te herstellen, dan moet het BCP een oplossing voorzien om tijdelijk, eventueel aan een gereduceerd niveau, toch de functionaliteit van de SPOF op te vangen voor het geval deze externe expertise door technische of praktische omstandigheden niet onmiddellijk beschikbaar is.

6.1.1.1. Motivatie

73. Proximus had voor de oplossing van het incident op 5 april 2019 de expertise nodig van de leverancier Nokia. Deze expertise kwam deels uit de Verenigde Staten.

74. Voor deze interventie was dus een goed werkende connectie tussen het netwerk van Proximus en het support center van Nokia vereist.

75. Op 5 april 2019 was er geen impact op de internetverbinding. Dit kan echter bij toekomstige incidenten niet uitgesloten worden. Het is daarom belangrijk dat Proximus in zijn BCPs rekening houdt met de mogelijkheid dat externe expertise niet onmiddellijk beschikbaar of bereikbaar is.

76. Proximus dient daarom te voorzien in een back-up-oplossing of -procedure om in dit geval de impact van een incident, al dan niet gedeeltelijk, zelf te kunnen opvangen.

6.1.2. Problemen op kritieke infrastructuur met de hoogste prioriteit behandelen

77. Problemen op onderdelen van kritieke infrastructuur dienen steeds met de hoogste prioriteit behandeld te worden. Dit geldt bijzonder in geval de oorzaak van de problemen onduidelijk is.

6.1.2.1. Motivatie

78. In de periode voorafgaan aan het incident waren er reeds enkele onverklaarbare problemen op de betrokken apparatuur.

79. Proximus had hiervoor een support-ticket aangemaakt bij de leverancier.

80. Aan dit ticket werd, achteraf gezien, niet de nodige prioriteit gegeven.

81. Tickets die van toepassing zijn op kritieke functies of componenten waarvan de onderliggende oorzaak onduidelijk is en de worst-case impact zeer groot dienen daarom met hoge prioriteit behandeld te worden.

6.1.3. Testen van de kritieke infrastructuur en de BCPs

82. Proximus dient de kritieke componenten en functies, alsook de bijhorende BCPs, op regelmatige basis testen zoals ook opgelegd door de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

6.1.3.1. Motivatie

83. In de context van wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, voert Proximus geregeld testen van de kritieke infrastructuren.

84. Deze testen hebben een grootschalige en langdurige impact op 5 april 2019 niet kunnen voorkomen.

85. Het is daarom essentieel dat deze testen aan de volgende voorwaarden voldoen:

    85.1. Ze moeten representatief zijn voor een reëel probleem.

    85.2. Niet enkel de technische herstelprocedure moet getest worden, ook de bijhorende BCPs in geval van bijkomende problemen tijdens het herstel moeten geregeld getest worden.

6.2. Aanbeveling op lange termijn

86. Zowel op fysiek als op logisch niveau raadt het BIPT Proximus sterk aan te streven naar een diversificatie voor kritieke netwerkcomponenten en -functies. Op deze manier kan de gelijktijdige uitval van hele componenten en -functies vermeden worden.

Axel Desmedt
lid van de Raad

Jack Hamande
lid van de Raad

Luc Vanfleteren
lid van de Raad

Michel Van Bellinghen
voorzitter van de Raad