REPUBLIKA E SHQIPËRISË
AUTORITETI I KOMUNIKIMEVE ELEKTRONIKE DHE POSTARE
Këshilli Drejtues

V E N D I M

Nr.2632, date 29.10. 2015

Për miratimin e dokumentit "Rregullore mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike" dhe përfundimin e këshillimit publik të realizuar për këtë dokument.

Këshilli Drejtues (KD) i Autoritetit të Komunikimeve Elektronike dhe Postare (AKEP), i përbërë nga:

1.	Z. Piro	Xhixho	Kryetar
2.	Z. Alban	Karapici	Anëtar
3.	Znj.Anila	Denaj	Anëtar
4.	Znj.Ketrin	Topçiu	Anëtar
5.	Znj. Klarina	Allushi	Anëtar

dhe sekretare Znj.Marsida Drushku, në mbledhjen e datës 29.10.2015, sipas procedurës së përcaktuar në ligjin nr.9918 datë 19.05.2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë" i ndryshuar, ligjin nr. 8480, datë 27.05.1999 "Për funksionimin e organeve kolegjiale të administratës shtetërore dhe enteve publike", dhe Rregullores së Brendshme të AKEP, miratuar me Vendimin Nr. 2506, datë 30.10.2014 të Këshillit Drejtues të AKEP, shqyrtoi çështjen me objekt:

Miratimin e dokumentit "Rregullore mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike" dhe përfundimin e këshillimit publik të realizuar për këtë dokument.

I.BAZA LIGJORE:

1. Ligji Nr 8485 datë 12.05.1999, "Kodi i proçedurave administrative" i ndryshuar;

2. Neni 6, neni 7 pika 1, gërma p) e nenit 8, neni 122 i Ligjit nr.9918, datë 19. 05. 2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar (ligji nr. 9918/2008);

4. Vendim nr.2592 datë 7 10.07.2015 për miratimin e dokumentit për këshillim publik "Rregullore mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike";

5. Rregullore e Brendshme e AKEP, miratuar me Vendimin Nr.2506, datë 30.10.2014 të Këshillit Drejtues të AKEP.

II. K Ë SH I LL I D R E J T U E S:

Nga shqyrtimi i materialit shkresor, të përbërë nga:

1. Dokumenti "Rregullore mbi sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike (Përmbajtja)
2. Relacioni shpjegues (Relacioni),
3. Përfundimet e Këshillimit Publik të realizuar për dokumentin sipërcituar,
4. Projekt Vendimi i formatuar dhe arsyetuar;

Diskutimeve në mbledhje mbi çështjen, si dhe duke iu referur bazës ligjore të sipërcituar,

III. V Ë R E N se:

1. Këshilli Drejtues i AKEP me Vendim nr.2592 datë 7 10.07.2015 vendosi të miratojë për Këshillim Publik projektaktin administrativ "Rregullore mbi sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike".

2. Dokumenti "Rregullore mbi sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike" është i hartuar në përputhje me kuadrin ligjor përkatës.

3. Dokumenti është përgatitur duke pasur në vëmendje përcaktimet e Nenit 13 a), Direktivë 2002/21 / EC të Parlamentit Evropian dhe e Këshillit, 7 Mars 2002 "Për një kuadër rregullator të përbashkët për rrjetet dhe shërbimet e komunikimeve elektronike (Direktiva Kuadër) amenduar me Direktivën 2009/140/EC të Parlamentit Evropian dhe Këshillit, të datës 25 nëntor 2009, Nenit 4 Direktivë 2002 / 58 / EC lidhur me përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike, (Direktivë e-Privacy) amenduar me Direktivën 2009/136/EC të Parlamentit Europian dhe Këshillit të datës 25.11.2009 dhe manualet guidë të ENISA.

4. Palët e interesuara, Vodafone Albania sh.a, Telekom Albania sh.a, Albtelekom sh.a dhe Plus Communication sh.a gjatë periudhës së Këshillimit Publik kanë depozituar në AKEP komentet mbi dokumentin për Këshillim Publik,

-Komente të sipërmarrësit Vodafone Albania datë 14.09.2015 me referencë LRD /0132/IK (AKEP shkresë Nr. Prot 992/4, datë 14.9.2015);

-Komente të sipërmarrësit Telekom Albania Nr.prot.4633 datë 11.09.2015 (AKEP shkresë Nr. Prot 992/6, datë 17.9.2015);

-Komente të sipërmarrësit Albtelecom datë 11.09.2015 nr. 7339 (AKEP shkresë Nr. Prot 992/5, datë 15.9.2015);

-Komente të sipërmarrësit Plus Communications datë 11.09.2015 nr.prot 1555 (AKEP shkresë Nr. Prot 992/3, datë 14.9.2015).

5. AKEP vlerëson komentet e palëve të interesuara në këtë këshillim publik dhe çmon si të arsyeshme miratimin e dokumentit "Rregullore mbi sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike dhe në zbatim pikës 4 të nenit 110 të Ligjit nr. 9918, datë 19.05.2008, i ndryshuar, Udhëzuesin e Procedurave për Këshillimin me Publikun miratuar me Vendim nr. 1183, datë 10.03.2010, publikimin e përfundimve të këtij këshillimi publik sipas dokumentit bashkëlidhur.

IV. PËR KËTO ARSYE:

Bazuar në sa më sipër, në kompetencat që i janë dhënë nga Ligji Nr 8485 datë 12.05.1999, "Kodi i proçedurave administrative" i ndryshuar, Ligji nr.9918, datë 19. 05. 2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar,

V. V E N D O S:

1. Të miratojë dokumentin "Rregullore mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike" dhe përfundimin e këshillimit publik, sipas dokumentit bashkëlidhur.

2. Të publikojë mendimet dhe komentet e palëve të interesuara, duke respektuar konfidencialitetin e informacionit, sipas dokumentit bashkëlidhur.

3. Ky Vendim dhe dokumenti "Rregullore mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike" të publikohet në faqen e internetit të AKEP www.akep.al.

Ky Vendim hyn në fuqi menjëherë.

K R Y E T A R

Piro XHIXHO

ANËTARËT E KËSHILLIT DREJTUES:

1. **Alban KARAPICI** _____
2. **Anila DENAJ** _____
3. **Ketrin TOPÇIU** _____
4. **Klarina ALLUSHI** _____

REPUBLIKA E SHQIPËRISË

AUTORITETI I KOMUNIKIMEVE ELEKTRONIKE DHE POSTARE

RREGULLORE

Nr 37 datë 29.10.2015

MBI MASAT TEKNIKE DHE ORGANIZATIVE PER TE GARANTUAR SIGURINE DHE INTEGRITETIN E RRJETEVE DHE/OSE SHERBIMEVE TE KOMUNIKIMEVE ELEKTRONIKE

Miratuar me Vendim të Këshillit Drejtues të AKEP nr.2632 datë 29.10.2015

Adresa: Rr. "Abdi Toptani", Godina Torre Drin, Kati IX, Tiranë
Tel : + 355 4 2259 571
Fax : + 355 4 2259 106
www.akep.al
info@akep.al

Neni 1

Dispozita të përgjithshme

Kjo Rregullore është hartuar në përputhje të Ligjit nr.9918, datë 19. 05. 2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar ***(ligji nr. 9918/2008***), Neni 6, gërma p) e nenit 8, neni 122.

Neni 2

Përkufizime

Përvec sa parashikohet në Ligjin nr.9918, datë 19. 05. 2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar ***(ligji nr. 9918/2008***), termat e meposhtëm do të kenë këto kuptime:

1. **"Incidenti i Sigurise"** Një shkelje e sigurisë ose një humbje e integritetit që mund të ketë një ndikim në funksionimin e rrjeteve dhe sherbimeve të komunikimeve elektronike.

2. **"Asetet e infrastruktures"** do te thote: Të gjitha pjeset e infrastruktures te ofruesit te rrjeteve dhe ose sherbimeve te komunikimeve elektronike te cilave, kur u cenohet integriteti dhe / ose dështojne ne funksionim, mund të kene një ndikim negativ në sigurinë apo vazhdimësinë e sherbimeve dhe rrjeteve të komunikimit elektronik apo shërbimeve.

3. **"Mohimi i Sherbimit -Denial of Service (DoS)" -** do te thote nderhyrje / veprime te jashtme drejt rrjetit te ofruesit te sherbimit, te cilat interferojne me punen e rrjetit te komunikimit publik dhe/ose sistemit te informacionit duke sjelle si pasoje mungese te sherbimeve per nje periudhe kohore.

4. **"Kompromentimi i Sistemeve te Informacionit"** do te thote perdorimi i jashteligjshem i burimeve te sistemeve te informacionit dhe/ose aksesi i pa autorizuar ne keto sisteme.

5. **"Software i Demshem (Malicious Software)"** do te thote nje software i plote ose nje pjese e tij e dizenjuar per tu lidhur me, ose per te mundesuar aksesin e pa autorizuar ne, sistemin e informacionit ose nje rrjet te komunikimit publik, modifikimin e operacioneve te sistemit te informacionit ose rrjetit te komunikimit publik, shkaterrimin, demtimin, fshirjen ose ndryshimin e te dhenave elektronike, eleminimin ose kufizimin e mundesise se perdorimit te te dhenave elektronike, qe con ne pervetesim ose perdorim nga persona, te paautorizuar per te pasur akses në keto të dhena.

6. **"Manipulimi i te Dhenave Elektronike"** do te thote shperdorimi dhe me tej perhapja dhe publikimi i te dhenave elektronike, zevendesimi i tyre me te dhena te tjere

elektronike, deformimi i te dhenave elektronike ose cdo perdorimin tjeter i jashteligjshem i tyre.

Neni 3

Qellimi

Kjo rregullore percakton detyrimin e sipermarresve që operojne nën regjimin e Autorizimit të Përgjithshem për ofrimin e rrjeteve dhe/ose shërbimeve publike të komunikimeve elektronike, që të marrin masat e duhura gjatë projektimit, instalimit dhe funksionimit të rrjetit ose pajisjeve të perdorura, në mënyrë që të garantojnë sigurinë, integritetin dhe funksionimin e rrjeteve të komunikimeve elektronike, si dhe te paraqesin prane AKEP, sipas Aneks nr.1 dhe Aneks nr.2, cdo nderhyrje, cenim ose incident ne sigurine dhe integritetin e rrjeteve te komunikimit elektronik publik qe ka nje impakt te konsiderueshem ne funksionimin e rrjeteve dhe/ose te sherbimeve te tyre.

Neni 4

Objekti

Kjo Rregullore synon:

a) Te percaktoje objektivat dhe masat per garantimin e funksionimit të infrastrukturës se rrjetit dhe/ose sherbimeve te komunikimit elektronik nga sipermarresit qe ofrojne akses ne rrjetet e komunikimit publik dhe /ose ne sherbimet e komunikimit publik, ne respekt te konfidencialitetit, integritetit dhe ofrimit te panderprere te sherbimeve.
b) Te percaktoje detyrimet dhe masat baze qe sipermarresit duhet te ndermarrin per te minimizuar apo parandaluar ndodhjen e incidenteve te sigurise ne rrjetet dhe/ose sherbimet e komunikimeve elektronike, dhe per ti raportuar ato nese ndodhin.
c) Kushtet qe duhet te plotesoje nje cenim ose incident sigurie, ne menyre qe te linde detyrimi i sipermarresit per te informuar AKEP ne lidhje me kete cenim ose incident sigurie.
d) Standardizimi në vleresimin dhe raportimin e incidenteve te sigurise dhe masave te sigurise te ndermarra nga sipermarresit.
e) Menyren dhe permbajtjen e raportimit te masave te sigurise dhe incidenteve te sigurise qe duhet dorezuar ne AKEP.
f) Percaktimi i sanksioneve, masave administrative ne rast se sipermarresit deshtojne ne permbushjen e detyrimeve te percaktuara ne kete rregullore.

Neni 5

Fusha e zbatimit

Percaktimet e kesaj rregulloreje jane te detyrueshme per tu zbatuar nga te gjithe sipermarresit e autorizuar nga AKEP të cilët ofrojne akses ne rrjetet apo sherbimet (fushen) e komunikimeve elektronike në përputhje me legjislacionin në fuqi.

Neni 6

Detyrimet e Sipermarresve

1. Sipërmarrësit duhet:

a) të informojnë AKEP brenda 3 ditëve pune, nese ndodh nje nga incidentet e meposhtme te sigurise:
   - Mohimi i Sherbimeve Elektronike
   - Kompromentimi i Sistemeve te Informacionit
   - Manipulimi ose modifikimi i paautorizuar i te Dhenave Elektronike
   - Software te demshem te cilet dergohen e jane nen kontrollin e drejtperdrejte te sipermarresit te komunikimeve elektronike (virus, spyware etj)

b) te informojne AKEP rreth incidenteve te zbuluara te sigurise dhe/ose cenimit te integritetit, te cilat kane pasur, kane ose mendohet se do te kene nje impakt te rendesishem dhe / ose mesatar ne ofrimin e rrjeteve te komunikimit publik dhe/ose ne sherbimet e komunikimit elektronik publik te perdoruesit, jo me vone se 24 ore nga evidentimi i incidentit.

c) te implementojne mjetet dhe metodat e duhura teknike dhe organizative per te garantuar sigurine e rrjeteve te komunikimit publik dhe te sherbimeve te ofruara prej tyre. Keto mjete duhet te garantojne nivelin e sigurise ne perputhje me rrezikun e paraqitur dhe te evitojne ndodhjen e incidenteve te sigurise ose te reduktojne impaktin ose pasojat kur keto incidente ndodhin.

d) te implementojne mjetet e duhura teknike dhe organizative per te garantuar integritetin e rrjeteve te komunikimit publik, duke siguruar ne kete menyre ofrimin e panderprere te sherbimeve te tyre.

e) te menaxhojne dhe mbrojne pajisjet dhe sistemet e perdorura per ruajtjen e te dhenave te perdoruesve te rrjeteve te komunikimit publik dhe/ose sherbimeve.

f) të sigurojnë një nivel të mbrojtjes dhe sigurisë së përshtatshme ndaj rreziqeve të mundshme, të parashikuara. Masat e ndermarra nga sipermarresit duhet që, të paktën:
   - të sigurojnë që të dhënat personale të jenë të aksesueshme vetëm nga personeli i autorizuar bazuar në legjislacionin përkatës;
   - të mbrojnë të dhënat personale të ruajtura ose të transmetuara nga aksidentet apo nga shkatërrimi i kundërligjshëm, humbja ose ndryshimi aksidental dhe ruajtja, përpunimi, aksesi apo zbulimi i paautorizuar ose i jashtëligjshëm;

- të sigurojnë implementimin e politikave të sigurisë, lidhur me përpunimin e të dhënave personale.

g) te kene rregullore ne lidhje me sigurine ose rregulla te mirepercaktuara, te publikuara dhe rregullisht te perditesuara per menaxhimin e rrjeteve dhe sherbimeve te komunikimeve elektronike publike.

h) te percaktojne minimalisht nje person te autorizuar qe do te jete pergjegjes per monitorimin e zbatimit te detyrimeve ne lidhje me sigurine, si dhe personi i kontaktit për komunikimin me AKEP ne rast të ndodhjes se nje incidenti sigurie.

i) detyrimisht duhet te kene planin e vazhdimesise se ofrimit te rrjeteve te komunikimit publik dhe/ose sherbimeve te komunikimeve publike, i cili do të aplikohet menjëherë ne momentin kur ndodh nje incident sigurie.

j) te publikojne ne website-t e tyre udhezues per perdoruesit rreth incidenteve me te zakonshme te sigurise, veprimeve dhe/ose mjeteve qe duhen ndjekur per te parandaluar ndodhjen e ketyre incidenteve dhe veprimeve qe duhen ndjekur pas ndodhjes se incidenteve te sigurise.

k) te informojne perdoruesit e sherbimeve te rrjeteve te komunikimit publik ne lidhje me punet e planifikuara per mirembajtje ose perditesime, të paktën 1 dite përpara fillimit të punimeve te cilat mund te sjellin nderprerje provizore te sherbimeve.

l) të informojnë përdoruesit e tyre për një rrezik të veçantë me impakt te larte ose mesatar, mënyrën se si rreziku mund të reduktohet nga përdoruesit, si dhe kostot e mundshme, që duhet të mbulohen nga përdoruesi, nëse rreziku që ndodh është jashtë masave, që mund të marrë sipërmarrësi.

2. Në rast të cenimit të të dhënave personale, sipërmarrësi që ofron shërbime të komunikimeve elektronike të vlefshme për publikun njofton AKEP për këtë shkelje jo me vone se 24 ore nga evidentimi i saj.

3. Kur një shkelje e të dhënave personale mund të ndikojë per keq ne te dhenat personale dhe privatësinë e pajtimtarit ose individit, sipërmarrësi, gjithashtu, njofton pajtimtarin ose individin për shkeljen jo me vone se 24 ore nga evidentimi i shkeljes.

4. Nëse sipërmarrësi i ka vërtetuar AKEP-it që i ka zbatuar masat e nevojshme mbrojtëse teknologjike dhe këto masa janë aplikuar për të dhënat përkatëse, atëherë nuk kërkohet nga sipërmarrësi të njoftojë pajtimtarin ose individin për shkeljen e të dhënave personale. Këto masa mbrojtëse teknologjike i bëjnë këto të dhëna të palexueshme për çdo person që nuk ka akses të autorizuar në këto të dhëna.

5. Pa paragjykim ndaj detyrimit të sipërmarrësit për të njoftuar pajtimtarët dhe individët në fjalë, nëse sipërmarrësi nuk e ka njoftuar pajtimtarin ose individin për shkelje të të dhënave personale, AKEP-i, pasi të ketë marrë parasysh ndikimin e shkeljes, mund të kërkojë që sipërmarrësi të njoftojë pajtimtarin.[1]

6. Njoftimi i pajtimtarit/ individit, përshkruan të pakten natyrën e shkeljes së të dhënave personale dhe personin e kontaktit ku mund të merret informacion më i detajuar, si dhe rekomandon masa për të minimizuar efektet e mundshme të këqija të shkeljes së të dhënave personale. Njoftimi për AKEP-in, përshkruan pasojat dhe masat e propozuara ose të ndërmarra nga sipërmarrësi për shkeljen e të dhënave personale.

7. Sipërmarrësit mbajnë një regjister/ evidenca të plota të shkeljeve të të dhënave personale, që përmban fakte lidhur me këto shkelje, ndikimin e tyre dhe masat e ndërmarra.

8. Sipermarresit qe ofrojne vete apo permes te treteve transaksione financiare online, duhet ti ushtrojnë ato ne perputhje me standartin PCI DSS (Payment Card Industry Data Security Standard).

Neni 7

Detyrimet e AKEP

1. Garanton ruajtjen e integritetit te te dhenave te sipermarresve te rrjeteve dhe/ose sherbimeve te komunikimeve elektronike publike nga modifikimet e tyre jo te autorizuara ose jo te kerkuara nga sipermarresi perkates.
2. Ushtron kompetencat ne perputhje me Ligjin e Mbrojtjes se te Dhenave Personale dhe aktet nënligjore në zbatim të tij.
3. Garanton ruajtjen e konfidencialitetit te te dhenave te sipermarresve te rrjeteve dhe/ose sherbimeve te komunikimeve elektronike publike prej personave jo te autorizuar me perjashtim te kerkesave që vijnë nga organe dhe institucione ne perputhje me legjislacionin në fuqi.
4. Investigon, nese e shikon te nevojshme, mbi incidentet e sigurise te raportuara nga sipermarresit duke ruajtur gjithmone sekretin dhe anonimatin e hetimit.
5. Njofton perdoruesit e rrjeteve dhe/ose sherbimeve te prekur, rreth incidentit te sigurise, në rast se e konsideron si te larte impaktin e incidentit te sigurise, duke vene ne dijeni sipermarresin e rrjetit ose sherbimit perkates.
6. Kryen kontrolle ne bashkepunim me ALCIRT, per te verifikuar implemetimin e kesaj rregulloreje ne rastet kur shihet e nevojshme.
7. Ndermerr masa sipas legjislacionit në fuqi nese sipermarresit nuk plotesojne kërkesat dhe kushtet e kesaj rregulloreje.

Neni 8

Vleresimi i Impaktit te Incidenteve te Sigurise

1. Sipermarresit duhet te kryjne vleresimin e impaktit te incidenteve te sigurise sipas tabeles se paraqitur ne Aneksin 2.

2. Incidentet e sigurise qe kane pasur kohezgjatje me pak se 1 ore, ne menyre automatike konsiderohen si te nje impakti te ulet dhe nuk eshte i nevojshem plotesimi i tabeles. Gjithashtu, incidentet e sigurise konsiderohen si incidente me impakt te ulet nese numri i perdoruesve te ndikuar nga incidenti eshte minimalisht sa 0.2% e numrit total te perdoruesve. por jo me shume se 1000.

3. Incidentet e sigurise konsiderohen si incidente me impakt te larte nese numri i perdoruesve te ndikuar nga incidenti ose perqindja e tyre (%) ndaj perdoruesve total eshte minimalisht 5% ose 1000 perdorues.

4. Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtrirjes se tij eshte minimalisht 20 km².

5. Ne cdo rast tjeter, incidentet e sigurise konsiderohen si incidente me impakt mesatar.

6. Ne vleresimin perfundimtar te impaktit te incidentit te sigurise, duhet patur parasysh se nese incidenti i sigurise eshte konsideruar i larte nga minimalisht 1 parameter (mesatar ose i ulet nga parametri tjeter), atehere ai konsiderohet nje incident me impakt te larte dhe ne vleresimin perfundimtar.

7. Tabela per vleresimin e impaktit te incidentit te sigurise mund te riplotesohet sa here qe kemi nje ndryshim te parametrave ne lidhje me kohezgjatjen e incidentit te sigurise, numrin e perdoruesve te prekur dhe zonen gjeografike te shtrirjes se incidentit te sigurise.

8. Brenda 30 diteve pune pas perfundimit te incidentit te sigurise, sipermarresit duhet te kryejne vleresimin perfundimtar te impaktit te incidentit te sigurise.

Neni 9

Raportimi i masave te sigurise dhe auditit

1. Te gjithe sipermarresit e shërbimeve te komunikimeve elektronike duhet te dergojne informacion te detajuar per te vleresuar sigurine dhe/ose integritetin e sherbimeve dhe rrjeteve ne AKEP periodikisht nje here ne vit, brenda muajit Janar per vitin paraardhes, sipas Aneksit 3 te kesaj rregulloreje.
2. Pas marrjes se informacionit sipas pikes 1 mesiper, nese AKEP vlereson se te dhenat dhe informacioni i depozituar kane nevoje per verifikime te metejshme te thelluara, ka te drejte ti kerkoje sipermarresve me te ardhura vjetore te vitit paraardhes nga komunikimet

elektronike nen vleren 100.000.000 leke, paraqitjen e Raportit me rezultatet e auditit te sigurise, te kryer nga nje organ i certifikuar dhe i pavarur i ose nga Autoriteti kompetent.

3. Sipermarresit e komunikimeve elektronike qe rezultojne sipas raportimeve te kryera ne AKEP, me të ardhura vjetore te vitit paraardhes nga komunikimet elektronike mbi vleren 100,000,000 leke, duhet qe te dorezojne prane AKEP raportin të sigurisë, të kryer nga një organ i certifikuar dhe i pavarur ose nga autoriteti kompetent. Raporti duhet te dorezohet periodikisht per nje periudhe jo me shume se dy vjecare
4. Kostoja e auditit te sigurise do të paguhet ne cdo rast nga sipërmarrësi.
5. Ne rast te shkeljes se sigurise ose kur auditi i sigurise zbulon masa jo te mjaftueshme te sigurise, AKEP-i me nje vendim detyron sipermarresit te zbatojne masat e nevojshme te sigurise. AKEP do te percaktoje kerkesat minimale per masat qe duhet te merren dhe afatet kohore per zbatimin e tyre

Neni 10

Raportimi i Incidenteve te Sigurise

1. Sipermarresit duhet te njoftojne dhe te dergojne formularin e Aneksit 1 prane Autoritetit jo me vone se 3 dite pune nga momenti i zbulimit te incidentit te sigurise. Kjo duhet bere vetem pas vleresimit te impaktit te incidentit te sigurise dhe vetem nese ai rezulton mesatar ose i larte.

2. Ky njoftim i pare duhet te permbaje te pakten informacionet e meposhtme:

a) vleresimin se cilat rrjete ose sherbime te komunikimit publik jane ndikuar ose do te ndikohen nga incidenti i sigurise,

b) vleresimin e zones gjeografike qe eshte ndikuar dhe/ose do te ndikohet nga incidenti i sigurise,

c) vleresimin e segmentit te perdoruesve qe jane ndikuar dhe/ose do te ndikohen nga incidenti i sigurise,

d) vleresimin e planit te rimekembjes,

e) vleresimin paraprak te shkakut ose shkaqeve, qe sipermarresi mendon se kane shkaktuar incidentin e sigurise.

3. Ne rastin ku ka nje ndryshim te rendesishem te te dhenave te percaktuara ne piken 2 te ketij neni, sipermarresi paraqet menjehere prane AKEP-it nje njoftim te ri.

4. Brenda 15 diteve pune nga ndodhja e incidentit te sigurise, sipermarresit duhet te paraqesin njoftimin perfundimtar, me te dhena me te plota, ne lidhje me incidentin e sigurise duke plotesuar perseri formularin e Aneksit 1. Njoftimi perfundimtar dergohet ne AKEP sipas percaktimeve te pikes 2 te ketij neni.

5. Njoftimi fillestar dhe perfundimtar dergohet ne AKEP permes emailt incidente.raportimi@akep.al dhe /ose permes instrumentave te tjere te vene ne dispozicion per kete qellim nga AKEP.

6. AKEP mund te kerkoj te dhena te tjera shtese, pervec atyre ne formularin perfundimtar, ne lidhje me incidentin e sigurise. Per kete arsye, sipermarresit jane te detyruar te ruajne te gjithe te dhenat ne lidhje me incidentet e sigurise te raportuara per nje periudhe kohore prej 12 muaj, qe nga koha e dorezimit te njoftimit perfundimtar rreth incidentit te sigurie.

Neni 11

Investigimi i Incidenteve te Sigurise dhe Cenimit te Integritetit

1. Duke vleresuar nivelin e impaktit te incidentit te sigurise dhe/ose cenimit te integritetit te raportuar sipas Formularit ne aneksin 1, AKEP mund te ndermarre veprimet e nevojshme per investigimin e ketij incidenti te sigurise dhe po ashtu per sqarimin e te gjitha rrethanave percaktuar nga njoftimi i sipermarresit.

2. Nese eshte e nevojshme, ne kuader te investigimit, AKEP do te informoje Agjensine Kombetare te Sigurise Kompjuterike (ALCIRT) dhe organet e tjera kompetente ne perputhje me legjislacionin për transmetimin e te dhenave nderkombetare.

3. AKEP-i, pasi ka marre vleresimin e impaktit te incidentit te sigurise nga sipermarresi, mund te informoje vete publikun, duke vene ne dijeni dhe sipermarresin, rreth incidentit te sigurise qe ka ndodhur, , ose te kerkoje nga sipermarresi qe ta njoftoje vete publikun, nese vlereson qe berja publike e kesaj shkeljeje eshte ne interes te publikut.

Neni 12

Zbatimi i rregullores

1. Te gjithe sipermarresit e komunikimeve elektronike publike janë të detyruar të zbatojnë kete rregullore.
2. Sipermarresit do te jene subjekt i masave administrative nese ne kundershtim me kete rregullore:
   a) nuk kane permbushur nje ose disa nga detyrimet e nenit 6;

b) nuk kane raportuar prane AKEP incidente te sigurise te nje impakti mesatar dhe/ose te larte;
c) nuk kane respektuar afatet e njoftimit dhe raportimit prane AKEP te incidenteve te sigurise;
d) kane bere nje vleresim jo te vertete te impaktit te incidentit te sigurise duke menjanuar ne kete menyre detyrimin e raportimit;
e) kane plotesuar formularin ne Aneks 1 me te dhena te rreme ose nuk e kane plotesuar ne menyre te plote;
f) nuk kane ruajtur te dhenat ne lidhje me incidentet e sigurise te raportuar per nje periudhe kohore prej 12 muaj qe nga koha e dorezimit te njoftimit perfundimtar rreth incidentit te sigurise.

3. Në mbështetje të nenit 135 të Ligjit Nr.9918, datë 19.5.2008 "Për komunikimet elektronike në Republikën e Shqipërisë" i ndryshuar, moszbatimi i detyrimeve qe rrjedhin nga kjo rregullore përbën kundravajtje administrative dhe në këto raste do të zbatohet legjislacioni në fuqi.

DISPOZITA KALIMTARE DHE TE FUNDIT

Neni 13

Informimi dhe publikimi

Kjo rregullore eshte pjesë e akteve rregullatore të nxjerra nga AKEP dhe publikohet në faqen e internetit të AKEP-it me hyrjen ne fuqi te saj.

Neni 14

Hyrja në fuqi

Kjo rregullore dhe Anekset e saj hyjne në fuqi pas miratimit me vendim të Këshillit Drejtues.

ANEKS 1

FORMULARI PER RAPORTIMIN E NJE INCIDENTI TE SIGURISE DHE/OSE CENIMIT TE INTEGRITETIT	
Informacion Kontakti	*Emri i Sipermarresit:*
	Emri dhe Mbiemri i personit te ngarkuar me eleminimin e incidenteve te sigurise dhe/ose cenimit te integritetit:
	Pozicioni i Punes:
	Adresa:
	Telefon, e-mail:
Pershkrimi i Incidentit te Sigurise dhe/ose Cenimit te Integritetit	*Lloji:*
	Percaktimi se cila rrjete, sisteme ose sherbime preken na incidenti i sigurise:

	Koha e ndodhjes dhe kohezgjatja:
	Informacion rreth shkakut fillestar ose shkaqeve:
	Pershkrimin e incidentit (percaktoni te dhenat ne menyre sa me te detajuar):
	Numri i perafert i perdoruesve te prekur nga incidenti i sigurise ose cenimi i integritetit ose perqindja e tyre(%) nga perdoruesve total te rrjetit dhe/ose sherbimit:
	Zona Gjeografike e prekur nga incidenti i sigurise dhe/ose cenimi i integritetit (km^2):

	Burimet e prekura
	Pasojat :
Menaxhimi i incidentit te sigurise dhe/ose cenimit te integritetit	*Veprimet e ndermarra(te planifikuara per tu ndermarre) per te eleminuar incidentin e sigurise dhe per te reduktuar pasojat e tij:* *Masat pas incidentit*
Informacione te Tjera te Rendesishme	*Mesimet e nxjerra*
Data	
Formulari depozitohet pranë Autoritetit Përgjegjës me:Fax:+355 4 2259 106 ose *E-mail (te skanuara) ne adresen: incidente.raportimi@akep.al*	

Fushat e Formularit të Raportimit të Incidenteve

Në këtë pjesë, do të përshkruhen fushat e raportimit të incidenteve, që duhet të përdoren nga Autoritetet Rregullatore kur dërgojnë raporte të incidenteve te ENISA dhe Komisioni Europian, si pjesë e raportimit përmbledhës vjetor.

Shërbimet e prekura

Në fushën "shërbimi i prekur", Autoritetet Rregullatore duhet të japin informacion se cila shërbime të komunikimeve elektronike janë prekur, për shembull duke përcaktuar një ose disa nga:

- Telefonia fikse
- Telefonia e lëvizshme
- Akses i internetit nëpërmjet rrjetit fiks
- Akses i internetit nëpërmjet rrjetit mobile

Ose në mënyrë alternative, autoritetet rregullatore mund të përcaktojnë se një lloj tjetër shërbimi është prekur. Po kështu, në mënyrë opsionale, autoritetet mund të japin informacione të mëtejshme rreth teknologjisë ose platformës së prekur.

Për shembull, nëse një stuhi rrëzon një numër të stacioneve bazë mobile, duke shkaktuar dëmtim të rrjetit, shërbimi i prekur në këtë incident do të jetë telefonia e lëvizshme, interneti nëpërmjet rrjetit mobile dhe vecanërisht GSM, GPRS/EDGE, UMTS, për të shpjeguar llojin e teknologjisë ose platformës së prekur.

Numri i përdoruesve

Në fushën "Numrin i përdoruesve", autoritetet rregullatore duhet të përcaktojnë numrin total të përdoruesve të prekur.

- Për telefoninë fikse dhe aksesin në internet nëpërmjet rrjetit fiks, autoritetet rregullatore duhet të raportojnë numrin e pajtimtarëve ose linjat e aksesit të prekura.
- Për telefoninë e lëvizshme dhe aksesin në internet nëpërmjet këtij rrjeti, autoritetet rregullatore duhet të raportojnë një vlerësim ose parashikim, duke marrë në konsideratë përdorimin normal të burimeve të prekura.

Për shembull, nëse një stacion bazë, i cili i shërben 1000 përdoruesve në orë mesatarisht, është jashtë shërbimit për një orë, atëherë impakti i këtij incidenti duhet vlerësuar si 1000 përdorues.

Duhet patur parasysh që në shumë incidente, disa shërbime janë të prekura në të njëjtën kohë dhe si pasojë numri i përdoruesve të prekur do të jetë i ndryshëm për cdo shërbim. Në këto raste, autoritetet rregullatore duhet të paraqesin të dhëna për cdo shërbim.

Duhet patur parasysh gjithashtu se ofruesit e shërbimeve, jo gjithmonë, kanë një përcaktim ekzakt të numrit të përdoruesve të prekur, sepse ata shpërndajnë shërbime në ofrues të tjerë (quhen shpesh rishitës, ose përdorues të ndërmjetëm). Ofruesi, në këtë rast, jo gjithmonë di numrin e saktë të përdoruesve (ose klientëve sic referohen në Direktivë) të fundit dhe rrjedhimisht nuk mund të njoh numrin e saktë të përdoruesve të prekur nga një incident. Në këto raste, autoritetet rregullatore duhet të raportojnë vlerësime ose parashikime.

Kohëzgjatja

Në fushën "kohëzgjatja", autoritetet rregullatore duhet të përcaktojnë afatin e kohës (në orë), gjatë të cilave ka patur impakt të rëndësishëm në funksionimin e shërbimeve.

Për shembull, supozojmë se një stuhi shkakton ndërprerje të energjisë elektrike nga mesnata deri në orën 6 të mëngjesit dhe supozojmë që shërbimi i telefonisë celulare preket nga ora 4 (kur energjia backup harxhohet) deri në 7 të mëngjesit. Në këtë rast, kohëzgjatja e incidentit është 3 orë.

Impakti në thirrjet e emergjences

Në fushën "impakti në thirrjet emergjente", autoritetet rregullatore duhet të përcaktojnë nëse ka patur një impakt në mundësinë për të telefonuar shërbimet e emergjencës, si ambulancën ose zjarrfikëset nëpërmjet numrave të emergjencës (112 në shumë vende).

Për shembull, supozojmë se qendra operative e një sipermarresi i telefonik ka një ndërprerje energjie, që pengon shumë zona të një vendi të lidhen me 112. Në këtë rast, incidenti ka një impakt në thirrjet e emergjencës.

Impakti në Interkoneksion

Në fushën "Impakti në Interkonjeksionet", autoritetet rregullatore duhet të përcaktojnë nëse ka ndonjë impakt në interkonjeksionet kombëtare dhe ndërkombëtare midis ofruesve.

Për shembull, supozojmë se një pikë e madhe shkëmbimi internet preket nga një ndërprerje e energjisë duke shkaktuar problem të mëdha të shërbimit internet. Në këtë rast, incidenti ka një impakt në interkonjeksionet.

Kategoria e shkakut fillestar

Shkaku kryesor i një incidenti është shkaku fillestar i incidentit, ose me fjalë të tjera, eventi ose faktori që nxiti incidentin. Në fushën "kategoria e shkakut fillestar", autoritetet rregullatore duhet të përcaktojnë kategorinë e shkakut fillestar, nxitës së incidentit. Kemi 5 kategori të shkakut fillestar:

Gabimet Njerëzore

Kategoria "gabimet njerëzore" duhet të përdoret për incidentet e shkaktuara nga gabimet njerëzore gjatë funksionimit të pajisjeve ose burimeve, përdorimin e mjeteve, ekzekutimin e procedurave etj.

Për shembull, supozojmë se një punonjës i një ofruesi kryen një gabim në procedurat e mirëmbajtjes së një pajisjeje duke shkaktuar mosfunksionimin e saj.Në këtë rast, incidenti duhet të jetë në kategorinë burimet njerezore si shkak fillestar ose nxitës i incidentit.

Dështimet e Sistemit

Kategoria 'Dështimet e Sistemit", duhet të përdoret për incidentet e shkaktuara nga dështimet e sistemit për shembull dështimet hardëare, softëare ose shkeljet e manualeve, procedurave ose politikave.

Për shembull, supozojmë se një ofrues ka një program të plotë mirëmbajtjeje për pajisjet e saj, dhe gjeneratorët diesel nuk janë të përfshirë në këtë program. Si pasojë, gjeneratori dështon për arsye se nuk ka një program mirëmbajtjeje për të. Në këtë rast, shkaku fillestar, nxitës i incidentit duhet të jetë në kategorinë e Dështimeve të Sistemit.

Dukuritë Natyrore

Kategoria "Dukuri Natyrore" duhet të përdoret për incidente që shkaktohen nga moti i përkeqësuar, tërmetet, përmbytjet, pandemitë, zjarret ose kafshët e egra etj.

Për shembull, supozojmë se ketrat presin kabllot, duke shkaktuar ndërprerje, atëherë incidenti duhet të jetë në kategorinë e shkakut fillestar si Dukuri Natyrore.

Veprimet e dëmshme

Kategoria "veprimet e dëmshme"duhet të përdoret për incidentet e shkaktuara nga veprimi i paramenduar i një personi ose i një grupi.

Për shembull, incidentet që kanë si arsye fillestare zjarrvënien nga punonjësit si një akt sabotazhi, ndërhyrja në sistemet DNS nga kriminelët, hack-imi i sistemeve kompjuterike të ofruesit e kështu me rradhë.

Dështimet e palëve të treta

Kategoria "dështime nga palë të treta", duhet të përdoret për incidente ku shkaku fillestar ose nxitës është jashtë kontrollit direkt të ofruesit, për shembull, kur shkaku fillestar ndodh te një kontraktor që përdoret për outsourcing ose te një organizatë furnitore.

Kjo kategori mund të përdoret më vete kur shkaku fillestar ose nxitës i incidentit është i panjohur. Në rastet e tjera, kjo kategori duhet të përdoret së bashku me një nga kategoritë e tjera të shkakut fillestar ose iniciues.

Për shembull, një ndërprerje e shkaktuar nga prerja e kabujve nga një makinë gërmimi gjatë ndërtimit të një rruge të re, mund të kategorizohet në kategorinë gabime njerëzore dhe dështime të palëve të treta.

Shkaku Fillestar

Në fushën "Shkaku Fillestar", autoritetet rregullatore duhet të përcaktojnë shkakun fillestar të incidentit, për shembull eventin ose faktorin që nxit incidentin.

Për shembull, shkaqet fillestare mund të jenë dështimet softëare, ndërprerjet e energjisë elektrike, sulmet kibernetike, harxhimi i karburantit backup e kështu me rradhë.

Duhet patur parasysh që këto shkaqe të detajuara mund të kategorizohen në kategori të ndryshme të shkakut nxitës, në varësi të specifikave të tij. Për shembull, një prerje kablli mund të shkaktohet nga një gabim njerëzor ose nga një defekt në procedurë.

Shkaqet e Tjera

Shpesh incidentet përfshijnë një sërë eventesh ose faktorësh. Në fushën "shkaku tjetër", autoritetet rregullatore mund të përcaktojnë një shkak (shih në listën e shkaqeve në sektorin 7.1.7), që ka luajtur një rol në incident.

Për shembull, një stuhi shkakton një ndërprerje të kabujve që sjell një ndërprerje të energjisë, kështu që në këtë rast shkaku fillestar është stuhia dhe shkaku tjetër ose pasues është ndërprerja e kabujve.

Burimet e Prekura

Autoritetet rregullatore duhet të përcaktojnë burimet ose asetet e prekura nga incidenti.

Për shembull, asetet e prekura mund të jenë stacionet bazë mobile, kabinat e rrugës, sëitchet, backbone ndërkombëtar e kështu me rradhë.

Përshkrimi i Incidentit

Në fushën "Përshkrimi i Incidentit", autoritetet rregullatore duhet të ofrojnë një përshkrim të incidentit dhe sesi u zhvillua në fillim.

Veprimet e përgjigjes ndaj incidentit

Në fushën "Veprimet e përgjigjes ndaj incidentit", autoriteti duhet të jap një përshkrim të veprimeve të ndërmarra nga ofruesi për të reduktuar impaktin e incidentit.

Masat pas incidentit

Në fushën "Masat pas incidentit", autoriteti duhet të ofroj një përshkrim të veprimeve ose masave të ndërmarra nga ofruesi për të reduktuar probabilitetin e ndodhjes ose impaktin e incidenteve të ngjashme në të ardhmen.

Mësimet e nxjerra

Në fushën "Përshkrimi i mësimeve të nxjerra", autoriteti duhet të vendos një përshkrim të mësimeve të nxjerra nga incidentet ose masave afatgjate që do të implementohen nga autoriteti ose ofruesit.

ANEKS 2

TABELA PER VLERESIMIN E IMPAKTIT TE INCIDENTIT TE SIGURISE		
Kohezgjatja e incidentit te sigurise(nderprerjes se sherbimit, interceptimit te komunikimeve, software te demshem, , modifikimi i te dhenave)	*Me teper se 1 ore, por me pak se 2 ore*	*Me teper se 2 ore*
Numri i perdoruesve te prekur nga incidenti ose % e tyre ndaj numrit total te perdoruesve te ofruesit		
>1000 ose >5%	*Mesatar*	*I Larte*
Ne rast te nje numri te panjohur te perdoruesve te prekur nga incidenti i sigurise, zona gjeografike e shtrirjes se incidentit te sigurise		
>20 km²	*Mesatar*	*I Larte*
Vleresimi Perfundimtar i Impaktit:	***Mesatar***	***I Larte***

ANEKS 3

Objektivat e Sigurisë dhe Mjetet

Më poshtë listohen 25 objektivat e nivelit të lartë të sigurisë (SO1, SO2 …), të grupuara në 7 fusha (D1, D2…). Për cdo objektiv të sigurisë, listohen masat e sigurisë që duhet të implementohen nga ofruesi i shërbimit për të plotësuar objektivin, po ashtu dhe faktet që duhen të merren në konsideratë nga një supervisor ose auditues kur vlerëson nëse mjetet apo masat mbrojtëse janë në funksion.

Më poshtë jepet një tabelë e përmbajtjes:

D1: Qeverisja dhe Menaxhimi i Riskut

SO 1: Politika e Sigurisë së Informacionit

SO 2: Qeverisja dhe Menaxhimi i Riskut

SO 3: Rolet e sigurisë dhe përgjegjësitë

SO 4: Siguria e aseteve të palës së tretë

D2: Siguria e Burimeve Njerëzore

SO 5: Kontrollet e Background-it

SO 6: Njohuria mbi sigurinë dhe trajnimi

SO 7: Ndryshimet e Personelit

SO 8: Trajtimi i Shkeljeve

D3: Siguria e sistemeve dhe pajisjeve

SO 9: Siguria Fizike dhe e Mjedisit

SO 10: Siguria e Burimeve

SO 11: Kontrolli i Aksesit në Rrjet dhe Sistemet e Informacionit

SO 12: Integriteti i Rrjetit dhe Sistemeve të Informacionit

D4: Menaxhimi i Operacioneve

SO 13: Procedurat Operacionale

SO 14: Menaxhimi I Ndryshimit

SO 15: Menaxhimi I Aseteve

D5: Menaxhimi I Incidenteve

SO 16: Procedurat e Menaxhimit të Incidenteve

SO 17: Aftësia e Zbulimit të Incidenteve

SO 18: Raportimi I Incidenteve dhe Komunikimi

D6: Menaxhimi I Vazhdimit të Biznesit

SO 19: Strategjia e Vazhdimit të Shërbimit dhe Planet e Emergjencës

SO 20: Aftësia e Rregullimit të Pasojave

D7: Monitorimi, Auditimi dhe Testimi

SO 21: Politikat e Logimit dhe Monitorimit

SO 22: Planet e Emergjencave

SO 23: Testimi I Rrjetit dhe Sistemeve të Informacionit

SO 24: Vlerësimet e Sigurisë

SO 25: Monitorimi I Pajtueshmërisë

D1: Qeverisja dhe Menaxhimi i Riskut

Fusha "Qeverisja dhe Menaxhimi i Riskut mbulon objektivat e sigurisë që lidhen me qeverisjen dhe menaxhimin e risqeve të sigurisë së rrjetit dhe informacionit.

SO 1: Politika e Sigurisë së Informacionit

Vendos dhe mbaj një politikë të duhur të sigurisë së informacionit.

	Masat e Sigurisë	Evidenca
1	a) Vendos një politikë sigurie të nivelit të lartë që adreson sigurinë dhe vazhdimësinë e rrjeteve të komunikimit dhe/ose shërbimeve të ofruara prej tyre.	• Politikë sigurie e dokumentuar, duke përfshirë rrjetet dhe shërbimet, burimet kritike mbështetëse të tyre dhe objektivat e sigurisë. • Personeli kyc është në dijeni të politikës së sigurisë dhe objektivave

	b) Vëje ne dijeni personelin kyc për politikën e sigurisë.	të tij (intervista).
2	c) Vendos politika të detajuara të sigurisë së informacionit për asetet kritike dhe proceset e biznesit. d) Vendos në dijeni gjithë personelin për politikën e sigurisë dhe për cfarë lidhet me punën e tyre. e) Rishiko politikën e sigurisë pas incidenteve nese konsiderohet e nevojshme.	• Politika të sigurisë së informacionit të dokumentuara të aprovuara nga menaxhimi, duke përfshirë ligjin dhe rregulloret e zbatueshme, të arrishme nga personeli. • Personeli është në dijeni të politikës së sigurisë së informacionit dhe për cfarë lidhet me punën e tyre (intervista) • Rishiko komentet ose ndrysho pjesë të politikës.
3	f) Rishiko politikat e sigurisë së informacionit në mënyrë periodike dhe merr në konsideratë shkeljet, përjashtimet, incidentet e mëparshme, testet/ushtrimet e mëparshme dhe incidentet që kanë prekur ofruesit e tjerë në sektor.	• Politikat e sigurisë së informacionit janë të përditësuara dhe të miratuara nga menaxhimi i lartë. • Mbajtje e përjashtimeve të politikës, të miratuara nga rolet e përshtatshme. • Dokumentimi i procesit të rishikimit, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.

SO 2: Qeverisja dhe Menaxhimi i Riskut

Vendos dhe mirëmbaj një strukturë të duhur të qeverisjes dhe menaxhimit të riskut për të identifikuar dhe adresuar risqet për rrjetet dhe shërbimet e komunikimeve.

	Masat e Sigurisë	**Evidenca**
1	a) Bëj një listë të risqeve kryesore për sigurinë dhe vazhdimësinë e rrjeteve dhe/ose shërbimeve të ofruara të komunikimit, duke marrë në konsideratë kërcënimet kryesore për burimet e rëndësishme. b) Vendos në dijeni personelin kyc për risqet kryesore dhe sesi ti trajtosh ato.	• Listë e risqeve kryesore të përshkruara në një nivel të lartë, duke përfshirë rreziqet themelore dhe impaktin e tyre potencial në sigurinë dhe vazhdimësinë e rrjeteve dhe shërbimeve. • Personeli kyc duhet të dijë risqet kryesore (intervista).
2	c) Krijo dhe vendos një metodologji të menaxhimit të riskut dhe/ose mjetet bazuar në	• Metodologji dhe/ose mjetet e menaxhimit të riskut të dokumentuara.

	standartet e industrisë. d) Siguro që personeli kryesor përdor metodologjinë dhe mjetet e menaxhimit të riskut e) Rishiko vlerësimet e riskut pas ndryshimeve ose incidenteve. f) Siguro që risqet e mbetura pranohen nga menaxhimi.	• Udhëzimi për personelin në vlerësimin e risqeve. • Listë e risqeve dhe evidencë e rishikimeve/përditësimeve. • Rishiko komentet ose ndryshimet në vlerësimet e risqeve. • Miratimi i menaxhimit për risqet e mbetura.
3	g) Rishiko metodologjinë dhe/ose mjetet e menaxhimit të riskut, në mënyrë periodike, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	• Dokumentim i procesit të rishikimit dhe përditësimeve të metodologjisë dhe/ose mjeteve të menaxhimit të riskut.

SO 3: Rolet e Sigurisë dhe Përgjegjësitë

Vendos dhe mirëmbaj një strukturë të duhur të roleve të sigurisë dhe përgjegjësive.

	Masat e Sigurisë	**Evidenca**
1	a) Caktoji personelit rolet e sigurisë dhe përgjegjësitë. b) Siguro që rolet e sigurisë janë të arritshme në rast se ndodhin incidente sigurie.	• Listë e roleve të sigurisë (CISO, DPO, menaxher i vazhdimësisë së biznesit, etj) të cilët dhe informacione kontakti.
2	c) Personeli emërohet zyrtarisht në rolet e sigurisë. d) Vendos personelin në dijeni të roleve të sigurisë në organizatë dhe kur duhet të kontaktohen.	• Listë e emërimeve (CISO, DPO,etj) dhe përshkrimi i përgjegjësive dhe detyrave për rolet e sigurisë(CISO, DPO, etj) • Materiale ndërgjegjësimi dhe informimi për personelin duke shpjeguar rolet e sigurisë dhe kur/si ata duhet të kontaktohen.
3	e) Struktura e roleve të sigurisë dhe përgjegjësive rishikohet rregullisht, si pasojë e ndryshimeve dhe/ose incidenteve të mëparshme.	• Dokumentim i përditësuar i strukturës së detyrave të roleve të sigurisë dhe përgjegjësive. • Dokumentim i procesit të rishikimit, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.

SO 4: Siguria e aseteve të palës së tretë

Vendos dhe mirëmbaj një politikë me kërkesa sigurie për kontratat me palët e treta për të garantuar që varësitë me palët e treta nuk ndikojnë negativisht sigurinë e rrjeteve dhe/ose shërbimeve.

	Masat e Sigurisë	Evidenca
1	a) Përfshini kërkesat e sigurisë në kontratat me palët e treat.	• Kërkesa të qarta të sigurisë në kontratat me palët e treat që na furnizojnë me produkte IT, shërbime IT, procese biznesi outsource, helpdesks, call center, ndërlidhje, pajisje të përbashkëta, etj.
2	b) Vendos një politikë sigurie për kontratat me palët e treta. c) Siguro që të gjitha prokurimet e shërbimeve/produkteve nga palët e treta janë në përputhje me politikën. d) Rishiko politikën e sigurisë për palët e treta, pas incidenteve ose ndryshimeve nese konsiderohet e nevojshme e) Redukto risqet e mbetura që nuk janë të adresuara nga pala e tretë.	• Politikë sigurie e dokumentuar për kontratat me palët e treta. • Listë e kontratave me palët e treta. • Kontratat për shërbime me palë të treta përmbajnë kërkesa sigurie në përputhje me politikën e sigurisë për prokurimet. • Rishiko komentet ose ndryshimet e politikës. • Risqet e mbetura që rezultojnë nga varësitë me palët e treta listohen dhe trajtohen.
3	f) Mbaj rekorde të incidenteve të sigurisë të lidhura ose të shkaktuara nga palët e treta. g) Rishikim dhe përditësim të politikës së sigurisë për palët e treta në intervale të rregullta, duke marrë në konsideratë incidentet dhe ndryshimet e mëparshme.	• Listë e incidenteve të sigurisë të lidhura ose të shkaktuara nga angazhimi me palët e treta. • Dokumentim i procesit te rishikimit të politikës.

D2: Siguria e Burimeve Njerëzore

Fusha Siguria e Burimeve Njerëzore mbulon objektivat e sigurisë që lidhen me personelin.

SO 5: Kontrollet e Background-it

Kryej kontrolle te duhura background mbi personelin (punonjësit, kontraktorët dhe përdoruesit e palëve të treta) nëse kërkohet për detyrimet dhe përgjegjësitë e tyre.

	Masat e Sigurisë	Evidenca
1	a) Kontrollo referencat	• Dokumentim i kontrollove të

	profesionale të personelit kyc(administratorit të sistemit, oficerëve të sigurisë, etj)	referencave profesionale për personelin kyc.
2	b) Kryej verifikime të background-it për personelin kyc, kur nevojitet dhe lejohet ligjerisht. c) Vendos një politikë dhe procedurë për kontrollet e background-it.	• Politikë dhe procedurë për kontrollet e background-it. • Udhëzim për personelin se kur/si të kryej kontrolle të background-it.
3	d) Rishiko dhe përditëso politikën/procedurat për kontrollet e background-it dhe referencës në mënyrë periodike, duke marrës në konsideratë ndryshimet dhe incidentet e mëparshme.	• Rishiko komentet ose ndryshimet e politikës/procedurës.

SO 6: Njohuria mbi sigurinë dhe trajnimi

Siguro që personeli ka njohuri të mjaftueshme mbi sigurinë dhe kryejnë trajnime të rregullta.

	Masat e Sigurisë	**Evidenca**
1	a) Garanto personelin kyc me trajnime dhe materiale të përshtatshme mbi cështjet e sigurisë.	• Personeli kyc ka ndjekur trajnime të sigurisë dhe ka njohuri të mjaftueshme mbi sigurinë (intervista).
2	b) Implemento një program për trajnimin, duke bërë të sigurt që personeli kyc ka njohuri të përditësuara dhe të mjaftueshme mbi sigurinë. c) Organizo trajnime dhe sesione ndërgjegjësimi për personelin në cështjet e sigurisë për organizatën.	• Personeli ka marrë pjesë në sesione ndërgjegjësimi në cështjet e sigurisë. • Program të dokumentuar për trajnimin mbi aftësitë e sigurisë, duke përfshirë objektivat për role të ndryshme dhe sesi të arrihen ato.
3	d) Rishiko dhe përditëso programin e trajnimit në mënyrë periodike, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme. e) Testo nivelin e njohurive mbi sigurinë të personelit.	• Program i përditësuar për ndërgjegjësimin dhe trajnimin mbi sigurinë. • Rezultatet e testeve mbi njohuritë e sigurisë të personelit. • Rishiko komentet ose ndryshimet për programin.

SO 7: Ndryshimet e Personelit

Vendos dhe mirëmbaj një process të duhur për menaxhimin e ndryshimeve në personel ose ndryshimet në rolet dhe përgjegjësitë e tyre.

	Masat e Sigurisë	Evidenca
1	a) Kur ka ndryshime në personel, hiq të drejtat e aksesit, badget, pajisjet, etj kur nuk nevojiten më. b) Eduko personelin e ri për politikat dhe procedurat.	• Evidencë që ndryshimet e personelit kanë pasuar me heqjen e të drejtave të aksesit, badget, pajisjet etj. • Evidencë që personeli i ri është edukuar rreth politikave dhe procëdurave.
2	c) Implemento politikë/procedura për ndryshimet e personelit, duke marrë në konsideratë heqjen në kohë të të drejtave të aksesit, badget, pajisjet. d) Implemento politikën/procedurat për edukimin dhe trajnimin për personelin në rolet e reja.	• Dokumentim të procesit të ndryshimeve të personelit, duke përfshirë përgjegjësitë për menaxhimin e ndryshimeve, përshkrimin e të drejtave të aksesit dhe posedimit të aseteve për cdo rol, procedurat për edukimin dhe trajnimin e personelit në rolet e reja. • Evidencë që ndryshimet e personelit janë kryer në bazë të procesit dhe që të drejtat e aksesit janë përditësuar në kohën e duhur.
3	e) Kontrolle periodike që politika/procedurat janë efektive. f) Rishiko dhe vlerëso politikën/procedurat për ndryshimet e personelit, duke marrë në konsideratë ndryshimet ose incidentet e mëparshme.	• Evidencë e kontrolleve mbi të drejtat e aksesit. • Politikë/procedura të përditësuara për menaxhimin e ndryshimeve në personel. • Rishiko komentet ose ndryshimet.

SO 8: Trajtimi i Shkeljeve

Vendos dhe mirëmbaj një process të disiplinuar për punonjësit që shkelin politikat e sigurisë ose një process më të gjerë që mbulon thyerjet e sigurisë të shkaktuara nga personeli.

	Masat e Sigurisë	Evidenca
1	a) Mbaj personelin të përgjegjëshëm për thyrjet e sigurisë të shkaktuara nga shkeljet e politikave, për shembull përmes kontratave të	• Rregulla për personelin, duke përfshirë përgjegjësitë, kodin e sjelljes, thyerjet e politikave etj, mundësisht si pjesë e kontratave të punës.

	punës.	
2	b) Vendos procedura për shkeljet e politikave nga personeli.	• Dokumentim i procedurës, duke përfshirë llojet e shkeljeve, që mund të jenë subjekt i masave disiplinore
3	c) Rishikim dhe përditësim periodik i procesit disiplinor duke u bazuar në ndryshimet dhe incidentet e mëparshme.	• Rishiko komentet ose ndryshimet.

D3: Siguria e Sistemeve dhe Pajisjeve

Kjo fushë "Siguria e Sistemeve dhe Pajisjeve"mbulon sigurinë fizike dhe logjike të rrjetit, sistemeve të informacionit dhe pajisjeve.

SO 9: Siguria Fizike dhe e Mjedisit

Vendos dhe mirëmbaj një siguri të duhur fizike dhe të mjedisit të rrjetit, sistemeve të informacionit dhe pajisjeve.

	Masat e Sigurisë	Evidenca
1	a) Elemino aksesin fizik të paautorizuar te pajisjet dhe infrastruktura dhe kryej kontrolle mjedisore për mbrojtjen ndaj hyrjes së paautorizuar, vjedhjes, zjarrit, përmbytjeve etj.	• Implementim bazë të masave të sigurisë fizike dhe kontrolleve mjedisore, si cëlsa, alarm ndaj vjedhjes, zjarrit, dhe sisitemin për shuarjen e tij etj.
2	b) Implemento një politikë të masave të sigurisë fizike dhe kontrolleve të mjedisit. c) Implementim i standarteve të industrisë mbi kontrollet fizike dhe të mjedisit.	• Politikë e dokumentuar për masat e sigurisë fizike dhe kontrolleve të mjedisit, duke përfshirë përshkrimin e pajisjeve dhe sistemeve. • Kontrolle fizike dhe të mjedisit, si kontrollin elektronik të hyrjes dhe mjete të gjurmimit, ndarje të hapësirave sipas niveleve të autorizimit, fikëse automatike zjarri etj.
3	d) Vlerëso efektivitetin e kontrolleve fizike dhe të mjeditit periodikisht. e) Rishiko dhe përditëso politikën për masat e sigurisë fizike dhe kontrollet e mjedisit duke	• Politikë e përditësuar për masat e sigurisë fizike dhe kontrollet e mjedisit. • Dokumentim të vlerësimit të kontrollit mjedisor, rishiko komentet ose ndryshimet.

	marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	

SO 10: Siguria e Burimeve

Vendos dhe mirëmbaj një siguri të duhur të burimeve (elektricitet, karburant etj)

	Masat e Sigurisë	Evidenca
1	a) Garanto sigurinë e burimeve si energjia elektrike, karburanti ose ftohësi.	• Siguria e burimeve mbrohet në një mënyrë bazike, për shembull përmes linjave backup të energjisë elektrike ose burimeve alternative të karburantit.
2	b) Implemento një politikë për sigurinë e burimeve kryesore, si energjia elektrike, karburanti etj. c) Implemento masat e sigurisë sipas standarteve të industrisë për të mbrojtur burimet dhe pajisjet.	• Politikë e dokumentuar për të mbrojtur burimet kryesore, duke përshkruar lloje të ndryshme të burimeve dhe masat e sigurisë për të mbrojtur këto burime. • Evidencë e masave sipas standartit të industrisë për të garantuar sigurinë e burimeve për shembull ftohjen, ristartim automatic pas ndërprerjeve të energjisë, gjeneratorët, bateritë etj.
3	d) Implemento masat e sigurisë për të mbrojtur burimet. e) Rishiko dhe përditëso politikën dhe procedurat rregullisht, duke marrë në konsideratë ndryshimet dhe incidentet dhe ndryshimet e mëparshme.	• Evidencë e masave për sigurinë e burimeve, si ftohjen active, UP, sistemet backup të energjisë etj. • Politikë e përditësuar për sigurinë e burimeve dhe pajisjeve mbështetëse, rishiko komentet ose ndryshimet.

SO 11: Kontrolli i Aksesit në rrjet dhe sistemet e informacionit

Vendos dhe mirëmbaj një kontroll aksesi logjik të duhur për aksesin në rrjet dhe sistemet e informacionit.

	Masat e Sigurisë	Evidenca
1	a) Përdoruesit dhe sistemet kanë identifikim unik dhe autentikohen kur aksesojnë shërbimet ose sistemet. b) Implemento mekanizmin e duhur të kontrollit logjik për	• Loget e aksesit tregojnë identifikues unik për përdoruesit dhe sistemet kur lejojnë ose mohojnë aksesin. • Përmbledhje e autentikimit dhe metodave të kontrollit të aksesit për sistemet dhe përdoruesit.

	rrjetin dhe sistemet e informacionit për të lejuar vetëm kontrollin e autorizuar.	
2	c) Implemento politikë për mbrojtjen e aksesit në rrjet dhe sistemet e informacionit, duke adresuar rolet, të drejtat, përgjegjësitë dhe procedurat për vendosjen dhe revokimin e të drejtave të aksesit. d) Zgjidh mekanizma të duhur të autentikimit në varësi të tipit të aksesit. e) Monitoro aksesin në rrjet dhe sistemet e informacionit, vendos një process të miratimit të përjashtimeve dhe regjistrimit të thyerjeve të aksesit.	• Politikë e kontrollit të aksesit duke përfshirë përshkrimin e roleve, grupeve, të drejtave të aksesit, procedurat për dhënien dhe revokimin e aksesit. • Tipe të ndryshme të mekanizmave të autentikimit për lloje të ndryshme të aksesit. • Loge të shkeljes së politikës të kontrollit të aksesit dhe përjashtimet të miratuara nga oficeri i sigurisë.
3	f) Vlerëso efektivitetin e politikave të kontrollit të aksesit dhe procedurave dhe implemento kontrolle në mekanizmat e kontrollit të aksesit. g) Politika dhe mekanizmat të kontrollit të aksesit rishikohen dhe kur nevojitet ndryshohen.	• Raporte të testeve të sigurisë të mekanizmave të kontrollit të aksesit. • Mjete për zbulimin e përdorimit jonormal të sistemeve ose sjelljeve jonormale të sistemeve (sistemet e zbulimit të ndërhyrjeve dhe anomalive). • Loge të sistemeve të zbulimint të ndërhyrjeve dhe anomalive. • Përditësime të politikës të kontrollit të aksesit, rishiko komentet ose ndryshimet.

SO 12: Integriteti i Rrjetit dhe Sistemeve të Informacionit

Vendos dhe mirëmbaj integritetin e rrjetit dhe sistemeve të informacionit dhe mbroji nga viruset dhe nga programet e tjera të dëmshme që mund të ndryshojnë funksionalitetin e sistemeve.

	Masat e Sigurisë	**Evidenca**
1	a) Siguro që programet e rrjetit dhe sistemet e informacionit nuk janë deformuar ose ndryshuar, duke përdorur kontrollin e inputeve dhe fireëall-et. b) Siguro që të dhënat kritike të	• Programet dhe të dhënat në rrjet dhe sistemet e informacionit mbrohen nëpërmjet kontrollit të inputeve, fireëall-et, enkriptimi dhe nënshkrimi. • Të dhënat kryesore të sigurisë mbrohen me mekanizma të mbrojtjes si memorje të shpërndarë, enkriptim,

	sigurisë si passëord-ët, sekretet, celsat privatë, nuk bëhën publike dhe as ndryshohen. c) Kontrollo për programme të dëmshme në rrjet dhe sistemet e informacionit.	hashing etj. • Sisteme të zbulimit të programeve të dëmshme janë prezente dhe të përditësuara.
2	d) Implemento masa sigurie sipas standarteve të industrisë, duke ofruar mbrojtje në thellësi ndaj modifikimit të sistemeve.	• Dokumentim sesi mbrojtja e programeve dhe të dhënave në rrjet dhe sisteme informacioni implementohet. • Mjete për zbulimin e përdorimit jonormal të sistemeve ose sjelljeve jonormale të sistemeve (si sistemet e zbulimit të ndërhyrjeve dhe anomalive). • Loge të sistemeve të zbulimit të ndërhyrjeve dhe anomalive.
3	e) Vendos kontrolle të mbrojtjes së integritetit të sistemeve. f) Vlerëso dhe rishiko efektivitetin e masave për të mbrojtur integritetin e sistemeve.	• Kontrolle të përditësuara për të mbrojtur integritetin e sistemeve, si nënshkrimi i kodit, etj. • Dokumentim të procesit të kontrollit të logeve për sistemet e zbulimit të ndërhyrjeve dhe anomalive.

D4: Menaxhimi i Operacioneve

Fusha "Menaxhimi i Operacioneve" mbulon procedurat operacionale, menaxhimin e ndryshimit dhe menaxhimin e aseteve.

SO 13: Procedurat Operacionale

Vendos dhe mirëmbaj procedurat operacionale për funksionimin e rrjetave dhe sistemeve të informacionit kryesore nga personeli.

	Masat e Sigurisë	Evidenca
1	a) Vendos procedura operacionale dhe përgjegjësi për funksionimin e sistemeve kritike.	• Dokumentim të procedurave operacionale dhe përgjegjësive për rrjetin dhe sistemet e informacionit kryesore.
2	b) Implemento një politikë për funksionimin e sistemeve për të garantuar që sistemet kryesore funksionojnë dhe menaxhohen sipas procedurave	• Politikë e dokumentuar për funksionimin e sistemeve kritike, duke përfshirë një përmbledhje të rrjetit dhe sistemev të informacionit.

	të paracaktuara.	
3	c) Rishiko dhe përditëso politikën/procedurat për funksionimin e sistemeve kritike, duke marrë në konsideratë incidentet dhe/ose ndryshimet.	• Politikë/procedurë të përditësuar për sistemet kritike, rishiko komentet dhe/ose ndryshimet.

SO 14: Ndryshimi i menaxhimit.

Krijimin e procedurave të menaxhimit të ndryshimit të rrjetit dhe sistemeve te informacionit kritike në mënyrë që të minimizohet mundësia e incidenteve që rezultojnë nga ndryshimet.

	Masat e Sigurise	Evidenca
1	a) Ndiqni procedurat e paracaktuara, kur bën ndryshime në sistemet kritike.	•Dokumentimi i ndryshimeve te procedurave te menaxhimit per sistemet kritike
2	b) Zbatimi i politikave / procedurave për menaxhimin e ndryshimeve, për të siguruar që ndryshimet e sistemeve kritike janë bërë gjithmonë duke ndjekur një mënyrë të paracaktuar. c) procedurat e menaxhimit të ndryshimit te dokumentit, dhe rekordet për secilen ndryshojnë sipas hapave të procedurës së ndjekur.	• Dokumentimi i ndryshimit i politikave të menaxhimit / procedurat e përfshira, sistemet nënshtrohen politikës, objektivat, rrokulliset përsëri procedurat, etj • Për çdo ndryshim, një raport është në dispozicion që përshkruan hapat dhe rezultat i ndryshimit
3	d) procedurat e menaxhimit të rishikimit dhe përditesimit ndryshojne rregullisht, duke marrë parasysh ndryshimet dhe incidentet e shkuara.	Proceduarat e menaxhimit te përditesimeve, të shqyrtojë komentet dhe / ose ndryshimi i logos.

SO: 15 Menaxhimi i burimeve

Vendosja dhe mirembajtja e procedurave te menaxhimit te burimeve dhe kontrolli i konfigurimit me qellim menaxhimin e gadishmerise te burimeve kritike dhe konfigurimi i rrjetit kritik dhe sistemit te informacionit.

	Masat e Sigurise	Evidenca
1	Menaxhimi i burimeve kritike dhe konfigurimi i sistemit kritik	• Lista e burimeve kritike dhe sistemit kritik
2	Implementimi i politikave / procedurave per menaxhimin e burimeve dhe kontrollin e konfigurimit.	• Politikat e dokumentura / procedurat per menaxhimin e aseteve , duke perfshire rregullat dhe pergjegjesite , burimeve dhe konfigurimet te cilat jane subject i politikave , objektivat e menaxhimit te aseteve
3	Rishikimi dhe perditesimi i herepashershem te politikave te menaxhimit te burimeve , bazuar ne ndryshimet dhe incidentet e shkuara	• Nje inventar burimesh ose inventare, te cilet permbajne burime kritike dhe varesine ndermjet aseteve • Nje inventar i kontrollit te konfigurimeve ose inventare , te cilet permbajne konfigurime te sistemit kritik. Perditesimin e politikave te menaxhimit / procedurave , rishikim te komenteve/ dhe / ose ndryshim i logs.

D5 : Menaxhimi i Incidenteve

Domain " Menaxhimi I incidenteve mbulon gjetjen e , pergjigjen e , raportimin e incidenteve dhe komunikimin ne lidhje me incidentet"

SO 16: Procedurat e menaxhimit te incidenteve

Vendosja dhe mirembajtja e procedurave per menaxhimin e incidenteve , dhe dergimi te personeli te duhur.

	Masat e Sigurise	Evidencat
1	a)Sigurimi qe personeli eshte ne gadishmeri dhe i pergatitur te menaxhoje dhe ti perballoje incidentet b)Te regjistroje incidentet kryesore	•Personeli te kuptoje si te veproje me incidentet dhe si ti pershkallezoje Inventarizimi i incidenteve kryesore dhe per incident, impaktin, shkakun veprimet e ndermarra , dhe mesimin e nxjerre
2	c)Implementimi i politikave/ procedurave per menaxhimin e incidenteve	•Politikat/ procedurat per menaxhimin e incidenteve , duke perfshire llojin e aksidentit qe mund te ndodhe , objektivat, rolin dhe pergjegjesite , pershkrim I detajuar, per tipin e incidentit, si ta menaxhojme incidentin, si te shkallzojme tek menaxheri etj
3	d)Investigimi i incidenteve kryesore dhe raportimi i tyre final, duke perfshire veprime te ndermarra dhe rekomandime per te zvogeluar incidente te ngjashme e)Vleresimi i politikave te menaxhimit te incidenteve / procedurave bazuar ne incidente te shkuara.	•Raporte individuale i perballimit te shumices se incidenteve Perditesimi i politikave te menaxhimit / procedurave , rishikim komentesh dhe/ ose ndryshim i logs.

SO 17 : Procesi e zbulimit te incidenteve

Krijon dhe miremban aftesine e zbulimit te incidenteve qe zbulon incidente

	Masat e Sigurise	Evidenca
1	a) Ngritja e proceseve apo sistemeve për zbulimin e incidentit.	• Incidentet e meparshme janë zbuluar dhe dërguar në kohë tek njerëzit e duhur.
2	b) Implementimi i sistemeve standarde të industrisë dhe procedurat për zbulimin e incidentit. c) Implementimi i sistemeve dhe procedurave për regjistrimin dhe përcjellja incidente ne kohë te njerëzit e duhur.	Sistemet dhe procedurat e zbulimit te incidentit, të tilla si incidentet e Sigurise dhe për Menaxhimin e Ngjarjeve (SIEM) mjete, Helpdesk siguri për personelin, raportet dhe advisories nga kompjuteri Ekipet emergjente Përgjigje (certs), mjetet për vend anomali, e të tjera.

3	d)Rishikimi i Sistemeve dhe procesit për zbulimin e incidentit rregullisht dhe përditësimin e tyre duke marrë parasysh ndryshimet dhe incidenteve të fundit. .	• Perditesimin e dokumentacionit të sistemeve të zbulimit incidenteve dhe proceseve. • Dokumentimi i rishikimit të procesit të zbulimit të incidentit, të shqyrtojë komentet, dhe / ose ndryshim i logs.

SO 18: Raportimi i incidentit dhe komunikimi

Vendos dhe mirembaj procedurat e raportimit dhe komunikimit per incidentet perkatese,duke marrë në llogari legjislacionin kombëtar të autoriteteve qeveritare në incidentin e raportimit.

	Masat e Sigurise	Evidenca
1	a)Të komunikojnë dhe të raportojnë në lidhje të vazhdueshme ose incidente të fundit të palëve të treta, konsumatorët, dhe / ose autoritetet qeveritare, kur është e nevojshme.	• Evidenca te komunikimeve te shkuara dhe raportime te incidenteve
2	Implementon politika dhe procedura per komunikimin dhe raportimin ne lidhje me incidentet	• Politika dhe procedurat për komunikimin dhe raportimin në lidhje me incidentet, duke e përshkruar arsyeve / motivimet për të komunikuar apo raportim (arsyet e biznesit, arsyet ligjore etj), lloji i incidenteve në fushëveprimin, përmbajtjen e kërkuar e komunikimit, njoftime dhe raporte të dokumentuara, kanalet që do të përdoren , dhe rolet përgjegjëse për komunikimin, njoftuar dhe raportimin. • Modele për raportim dhe komunikim e incidentit
3	c) Vlerësoni komunikimet e shkuara dhe raportimin në lidhje me incidentet. d) Rishikimi dhe përditësimin e planeve të raportimit dhe komunikimit, bazuar në ndryshimet apo incidenteve të fundit.	• Lista e raporteve të incidenteve dhe të komunikimit të fundit në lidhje me incidentet • Deri në përgjigje të incidentit dhe politikës së komunikimit, të shqyrtojë komentet, dhe / ose ndryshim i logs.

D6: Menaxhimi i Vazhdimit të Biznesit

Domain "Menaxhimi i vazhdimit te Biznesit" mbulon vazhdimësinë e strategjitve dhe planeve te emergjences për te zbutur deshtimet e medha dhe /ose të fatkeqësive natyrore

SO 19: Strategjia e Vazhdimit të Shërbimit dhe Planet e Emergjencës

Të krijojë dhe mirëmbajë plane emergjente dhe një strategji për të siguruar vazhdimësinë e rrjeteve dhe shërbimeve të komunikimit të ofruara.

	Masat e Sigurise	Evidenca
1	a) Implemento një strategjie ne vazhdimësinë e shërbimi për rrjetet e komunikimeve dhe / ose shërbimeve të ofruara.	• Strategji te dokumentuar per vazhdimësinë e shërbimit, duke përfshirë objektivat kohë për shërbimet kryesore dhe proceseve.
2	a) Zbatimi plane rezervë për sistemet kritike. b) Aktivizimin i monitorimit dhe zbatimin e planeve të paparashikuara, regjistrimi herëve të suksesshme dhe të kohes se dështimit.	•Plane emergjence për sistemet kritike, duke përfshirë hapa te qarta dhe procedurat për kërcënimet e njohura, shkaktuesit për aktivizimin, hapat dhe objektivat kohore • Procesi i vendimit për aktivizimin e planeve të emergjente. • Shkrime të aktivizimit dhe të ekzekutimit të planeve emergjente, duke përfshirë vendimet e marra, hapat e ndjekur, koha e rregullimit final.
3	d) Rishikimi e sherbimeve strategjike ne menyre te vazhdueshme dhe periodikisht d) Rishikimin plane emergjence, bazuar në incidentet e fundit dhe ndryshimet.	• Perditesimi i strategjise ne vazhdueshmeri dhe planin e incidenteve, rishikim komentesh, dhe /ose ndryshim i logs.

SO 20: Kapacitetet per rimekembjen nga katastrofat ne rrjet

Vendos dhe mirëmbajë e kapaciteteve te duhura per rimekembjen dhe rikthimin ne gjendje normale te rrjetit dhe sherbimeve te tjera te komunikimit ne rastet e katastrofave natyrale ose/dhe te me pasoja e medha.

	Masat e Sigurise	Evidenca
1	a) Pergatitja per rikthimin ne gjendje normale e sherbimeve ne katastrofen e rradhes	Permasat merren gjithmone ne lidhje me situaten, si p.sh failover ne zona te tjera pervec rrjetit akual qe po perdoret, backup I te dhenave kritike ne distanca te largeta etj.

2	b) Implementimi i proçedurave/policive per efektivitetin sa me te larte te kapaciteteve per rimekembjene e situates c) Implementimi I kapaciteteve te industrive standarte te rimekembjes se katastrofave ose te perdorin pale te treta (siç jane rrjetet emergjente nacionale)	Proçedurat/policite Documented policy/ per efektivitetin sa me te larte te kapaciteteve per rimekembjene e situates, duke perfshire nje liste te katastrofave natyrale qe mund ndikojne ne sherbime, dhe nje liste te kapaciteteve (ato nga palet e treta por edhe ato te brendshem) Implementimin e industrive standarte per kapacitetet e rimekembjes , siç jane pajisjet mobile, sitet mobile, sitet failover etj.
3	c) Vendosja e nje mekanizmi per mitigimin kapaciteteve per rregullimin e situates d) Kontrollimi dhe updatimi I kapacatiteve en menyre te vazhdueshme te regullt, duek amrre parasysh ndryshimet qe ndodhin, incidentet e meparshme, rezultatet e testeve.	Ky lloj mekanizmi perfshin te gjithe mekanizmat failover paandalues per katastrofat natyrale me pasoja te medha Dokumentimi i kapaciteteve per rregullimin e situates ne fjale , te shikohen komentet dhe/ ose ndryshim i logs.

D7: Monitorimi, Auditimi dhe Testimi

Domaini "Monitorimi, auditimi dhe testimi" mbulon monitorimin, testimin dhe auditimin e rrjetit dhe sistemeve informatike duke na dhene shume thjeshtime.

SO:21 Politikat e Logi dhe Monitorimit

Vendos dhe mirëmbajë sistemet dhe funksionet për monitorimin dhe logeve te rrjeteve kritike dhe sistemeve te komunikimit.

	Masat e Sigurise	Evidenca
1	a)Imlementimin e monitorimit dhe logeve e sistemeve kritike	•Loget dhe raportet e monitorimit të rrjetit kritik dhe të sistemeve te informacionit.
2	b) Implementon politikën e ngjarjeve dhe monitorimin e sistemeve kritike. c) Vendos mjete për monitorimin e sistemeve kritike d) Vendos mjetet për të mbledhur dhe ruajtur shkrimet e sistemeve kritike.	•Politika te dokumentuara për monitorimin dhe ngjarjet, duke përfshirë kerkesat minimale per monitorimin dhe ngjarjet, periudhën e mbajtjes, dhe objektivat e përgjithshme të ruajtjes monitoringdata dhe shkrimet. • Mjetet për sistemet e monitorimit dhe

		mbledhjen e logot
3	e) Vendos mjetet për mbledhjen dhe analizën e të dhënave të monitorimit dhe logot. f) Rishikimi dhe perditesimin i ndodhive dhe monitorimin e politikave / procedurave, duke marrë parasysh ndryshimet dhe incidenteve te shkuara.	•Mjete për të lehtësuar regjistrimin strukturor dhe analizën e monitorimit dhe logot. • Përditësuar dokumentacionin e monitorimit dhe politikat e ngjarjeve / procedurat, të shqyrtojë komentet, dhe / ose ndryshim i logs

SO:22 Qeverisja dhe Menaxhimi i Riskut

Vendos dhe mirëmban politika për testimin dhe ushtrimin *backup* dhe të planeve emergjente, ku nevojitet bashkëpunim me palët e treta.

	Masat e Sigurise	Evidenca
1	a) Veprime dhe backup provë dhe planet emergjente për t'u siguruar që sistemet dhe proceset e punës dhe personeli është i përgatitur për dështimet e mëdha dhe të paparashikuara.	•Raportet e veprimeve te fundit të backup dhe të planeve emergjente.
2	b)Implementimi i programit për ushtrimin backup dhe planeve emergjente rregullisht, duke përdorur skenare realiste që mbulojnë një gamë të skenarëve të ndryshëm gjatë kohës. c) Sigurohuni që çështjet dhe mësimet e nxjerra nga ushtrimet janë adresuar nga njerëzit përgjegjës dhe se proceset dhe sistemet përkatëse janë përditësuar në përputhje me rrethanat.	•Programet e veprimit per backup dhe plane emergjente duke perfshire llojet e papritura , frekuencën, rolet dhe përgjegjësitë, modelet dhe procedurat për kryerjen e ushtrimeve, modele për raportet e ushtrimit. • Raportet mbi ushtrimet dhe testimet tregon ekzekutimin e planeve emergjente, duke përfshirë mësimet e nxjerra nga ushtrimet. • Çështjet dhe mësimet e nxjerra nga ushtrimet e shkuara kanë qenë të drejtuar nga njerëzit përgjegjës.
3	d) Rishikimi dhe përditësimin e planeve te ushtrimit, duke marrë parasysh ndryshimet dhe incidentet e shkuara dhe të paparashikuara të cilat nuk janë të mbuluara nga programi i veprimit.	• Perditesimi i planeve te ushtrimit, të shqyrtojë komentet, dhe / ose të ndryshojë logot. • Input nga furnizuesit dhe palët e tjera të treat përfshira për mënyrën se si të përmirësojme

	d) Përfshirja furnizuesit, si dhe palët e tjera të treta, si partnerët e biznesit ose konsumatorët në veprim.	skenarin e ushtrimeve.

SO 23: Rrjeti dhe testimi i sistemit te informacionit

Vendos dhe mirëmbajë rregulla për testimin e rrjetit dhe sistemet e informacionit, veçanërisht kur lidhja eshte me rrjete ose sisteme te reja.

	Masat e Sigurise	Evidenca
1	a)Testo rrjetet dhe sistemet e informacionit perpara se ti perdorni ato ose ti lidhni me sistemet egzistuese.	•Testo raportet e rrjetit dhe sistemeve te informacionit, duke perfshire testet pas ndryshimeve te medha ose prezantimit te sistemeve te reja.
2	b) Implemento rregulla dhe procedura per te testuar rrjetin dhe sitemet e informacionit, c)Implemento vegla per testime automatike	•Rregullat/procedurat per testimin e rrjeteve dhe sistemeve te informacionit, duke perfshire kur tested duhet te behen, planifikimi i testeve, rasted e testeve, tabela shembull boshe te rraporteve te testeve.
3	c)Rishikimi dhe azhurnimi i rregullave / procedurat për testim, duke marrë parasysh ndryshimet dhe incidentet e fundit.	•Lista e raporteve të testimit. • Rregullat /procedurat e permirsuara te reja për testimin e rrjeteve dhe sistemet e informacionit, të shqyrtojë komentet, dhe / ose dokumentin (logun) i ndryshimeve.

SO 24: Vleresimi i Sigurise

Vendosja dhe mirëmbajtja e përshtatshme e politikave për kryerjen e vlerësimeve të sigurisë të rrjetit dhe të sistemeve te informacionit.

	Masat e Sigurise	Evidenca
1	a) Siguro qe sistemet kritike tu nënshtrohen sigurisë se canimeve dhe testimin e sigurisë	•Raporto nga scanimet e sigurise se meparshme dhe testet e sigurise.

	rregullisht, sidomos kur sistemet e reja janë futur dhe ndiqen ndryshimet. .	
2	b) Implemento rregulla/procedura për vlerësimin e sigurisë dhe testimin e sigurisë.	•Rregullat / Procedurat e dokumentuara për vlerësimin dhe testimin e sigurisë, duke përfshirë, cilat asete, në çfarë rrethanash, lloji i vlerësimeve të sigurisë dhe testet, frekuenca, palet e miratuara (të brendshme ose të jashtme), nivelet e konfidencialitetit për vlerësimin dhe rezultatet e testimit dhe vlerësimet e objektivave të sigurisë dhe testet.
3	c) Vlereso efektivitetin e politikave / procedurave për vlerësimin dhe testimin e sigurisë. d) Shqyrto dhe korrigjo politikat / procedurat për vlerësimin dhe testimin e sigurisë, duke marrë parasysh ndryshimet dhe incidenteve të shkuara.	•Lista e raporteve per vleresimin dhe testimin e sigurise. •Raportet e veprimive te ndermarra në vlerësimin dhe rezultatet e testimit •Ndrysho rregullat / procedurat për vlerësimin dhe testimin e sigurisë,shqyrto komentet, dhe / ose ndryshim i logs.

SO 25: Monitorimi i pajtueshmerise – Monitorimi i rregullt sipas ligjit

Vendosja dhe mirmbaje e politikave per monitorimin e pajtueshmerise me standarte dhe kerkesat ligjore.

	Masat e Sigurise	Evidenca
1	a) Monitoro zbatimin brenda standardeve dhe kërkesave ligjore	•Raporte qe pershkruajne rezultatin e zbatimit monitorimit
2	b) Implemento rregulla dhe procedura per monitorimin e rregullt dhe auditimin	•Rregullat / Procedurat e dokumentuara për monitorimin e zbatimit te rregullt dhe auditimit, duke përfshirë edhe (aktiveve, proceset, infrastruktura), frekuencat, udhëzimet që duhet të kryejnë auditime (te brendshme- ose të jashtme), rregullat përkatëse të sigurisë që janë objekt i monitorimit të pajtueshmërisë dhe auditimit, objektivat dhe synimet e nivel të lartë të monitorimit të pajtueshmërisë dhe auditimit, templeta(rregjistra) për raportet e auditimit.

		•Monitorime te detajuara dhe plane auditimi duke perfshire objektive dhe planifikim te nivelit te larte dhe afatgjate.
3	c)Vlerësoni politikat / procedurat sipas standarteve dhe auditim d) Rishikimi dhe perditesimi i politikave/ procedurat për pajtim dhe të auditimit, duke marrë parasysh ndryshimet dhe incidenteve të fundit.	•Lista e të gjitha raporteve dhe ankesave të pajtueshmërisë dhe auditimit •Rregullat e perditesuara/ procedurat e e ankuara dhe auditimin, shqyrtimi i komenteve, dhe / ose të ndryshimi te logos.

REPUBLIKA E SHQIPËRISË
AUTORITETI I KOMUNIKIMEVE ELEKTRONIKE DHE POSTARE

Përfundime të Këshillimit Publik

Në përfundim të procesit të Keshillimit Publik te realizuar për dokumentin **"Rregullore mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike"** u administruan dhe shqyrtuan komentet si më poshtë vijon:

- Komente të sipërmarrësit A datë 14.09.2015 me referencë LRD /0132/IK (AKEP shkresë Nr. Prot 992/4, datë 14.09.2015);

- Komente të sipërmarrësit B Nr.prot.4633 datë 11.09.2015 (AKEP shkresë Nr. Prot 992/6, datë 17.9.2015);

- Komente të sipërmarrësit C datë 11.09.2015 nr. 7339 (AKEP shkresë Nr. Prot 992/5, datë 15.9.2015);

- Komente të sipërmarrësit D datë 11.09.2015 nr.prot 1555 (AKEP shkresë Nr. Prot 992/3, datë 14.9.2015).

Neni 1

Nuk ka

Neni 2

Sipërmarrësi A

A sugjeron qe perkufizimet ne kete nen te jene ne perputhje me standardet perkatese nderkombetare dhe manualet guide te Enisa. Ne kete kontekst sugjerojme qe perkufizimi lidhur me "Mohimin e sherbimit - denial of service" te riformulohet duke saktesuar se mohimi i sherbimit quhet i tille atehere kur shkaktohet nga nderhyrje/veprime te jashtme dhe jo te brendshme te operatorit.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e operatorit A ne lidhje me perkufizimin ne nenin 2, pika 3 "Mohimi i Sherbimit".

Lidhur me perkufizimin e "incidentit te sigurise", ne perputhje me Ligjin 9918/2008, neni 122, si dhe Rregulloren per Autorizimin e Pergjithshem dhe detyrimet perkatese qe lindin nga Autorizimet e Pergjitshme te leshuara nga AKEP, masat teknike dhe organizative per te realizuar sigurine e rrjeteve dhe/ose te sherbimeve te ofruara prej tyre lidhen me garantimin e sherbimit qe operatoret e komunikimeve elektronike publike I ofrojne publikut. Ne perputhje me kuadrin ligjor si me lart, A

vlereson se "Incident i sigurise" ne kete Rregullore duhet te quhet shkelja e evidentuar e sigurise ose humbja e integritetit te rrjetit e cila afekton sherbimin e komunikimit elektronik publik (thirrje, SMS. MMS, internet) ndaj paitimtareve fundore dhe te dhenave e tyre personale, qe ka lidhje te drejtperdrejte me ofrimin e rrjeteve dhe sherbimeve nga operatori i komunikimeve elektronike, si dhe persa eshte nen kontrollin normal te operatorit te komunikimeve elektronike ne perputhie me detyrimet ligjore dhe te rregullores per autorizimin e pergjithshem. Ne kete kuptim, "Incidenti i sigurise" per qellimin e kesaj Rregullore nuk duhet te perfshije shkeljet e sigurise dhe humbja e integritetit qe lidhet me sistemet e sherbimet e brendshme te kompanise qe nuk kane lidhje me pajtimtaret fundore, si dhe shkeljet e sigurise qe mund te shkaktohen nga pale te treta te cilat kontaktojne drejtperdrejt perdoruesin e internetit pa nderhyrjen e operatorit te komunikimeve elektronike.

Qëndrimi i AKEP:
AKEP i qendron perkufizimit te gjendur, pasi eshte ne perputhje me percaktimet e ENISA ne "Article 13a Technical Guideline On Security Measures" dhe behet fjale per ato incidente te cilat kane ndikim në funksionimin e rrjeteve dhe sherbimeve të komunikimeve elektronike dhe te dhenat e pajtimtareve.

Sipërmarrësi B

Pika 2.1. Integriteti duhet të specifikohet si term më vete.

Qëndrimi i AKEP: *Komentet e operatorit B jane ne perputhje me percaktimet e rregullores, neni2, pika 1.*

Neni 3

Sipërmarrësi A

Neni 3 "Qellimi": Si edhe me lartpermendur lidhur me perkufizimin e "Incidentit te sigurise", ne perputhje me ligjin 9918/2008, neni 122, si dhe Rregulloren per Autorizimin e pergjithshem, A propozon qe qellimi i kesaj Rregulloreje te saktesohet sa i perket garantimit te sigurise, integritetit dhe funksionimit te rrjeteve sistemeve te komunikimit elektronik qe kane lidhje me ofrimin nga operatoret qe operojne nen regjimin e Autorizimit te Pergjithshem, te sherbimeve te komunikimeve elektronike (voice. SMS, MMS. Internet) per publikun dhe kane te dhena personale, per aq sa eshte nen kontrollin e ligjshem te operatoreve.

Qëndrimi i AKEP:
AKEP i qendron percaktimit te nenit 3 te rregullores pasi nuk shikohet e nevojshme cilesimet ne lidhje me llojet e sherbimeve (voice. SMS, MMS. Internet) dhe ne lidhje me kontrollin e ligjshem te operatoreve. AKEP nuk mund te dale jashte percaktimeve ligjore te detyrueshme per operatoret.

Neni 4

Sipërmarrësi A

Per te njejten arsye si me lart, propozojme qe pika a) e nenit 4 te rregullores te saktesohet duke shtuar pas fjalise se fundit: dhe ofrimit te panderprere te sherbimeve te komunikimeve elektronike (voice, SMS. MMS, intemet) perpublikun nga operatoret qe operojne nen regjimin e Autorizimit te pergjithshem, per aq sa eshte nen kontrollin e ligjshem te operatoreve"

Qendrimi i AKEP:
AKEP vlereson se nuk eshte e nevojshme te cilesohet pasi eshte e qarte dhe nenkuptohet se AKEP nuk mund te kerkoje me teper se sa eshte nen kontrollin e ligjshem te operatoreve.

Sipërmarrësi B

Pika (f), Përcaktimi i sanksioneve, masave administrative në rast se operatorët dështojnë në përmbushjen e detyrimeve të përcaktuara në këtë rregullore.

Komenti i B: Masat ndëshkimore duhet të bazohen në afatet që duhet të kenë Operatorët në implementimin e këtyre kërkesave. Ky dokument duhet të saktesojë qartë afatin kohor që do të kenë Operatorët për të implementuar këto kërkesa mbasi ky dokument të hyjë në fuqi. Nëse Operatori njofton AKEP për vështirësitë teknike që mund të ketë gjatë implementimit të këtyre kërkesave a do të ketë përsëri penalizim.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e ardhur nga B , mbi percaktimin e afatit kohor per permbushjen e detyrimeve qe rrjedhin nga kjo rregullore. Percaktimet mbi keto afate parashikohen ne neni nr.13 "Dispozite Kalimtare"

Neni 5

Nuk ka

Neni 6

Sipërmarrësi A

Ne vijim, ne nenin 6 pika 1, lidhur me detyrimin per njoftimin e AKEP per "Software te demshem" (Spam, virus, spyware..) kur keto dergohen permes internetit nga pale te treat, pa lidhje me operatorin e rrjetit dhe sherbimeve te komunikimeve elektronike; Ne perputhje me 2 nga 6 Ligjin 9918/2008, nenet 121,123, operatoret e komunikimeve elektronike kane detyrim ligjorte respektojne fshehtesine dhe konfidencialitetin e komunikimit elektronik dhe te mos interceptojne permbajtjen e komunikimit te perdoresve te rrjeteve dhe sherbimeve te tyre. Ne kete kuptim, sa i perket mesazheve me permbajtje malware qe mund te shperndahen permes internetit nga pale te treta pa lidhje me operatorin, A vlereson se operatoret e kane te ndaluar ligjerisht qe te identifikojne paraprakisht nje mesazh te tille, e per rrjedhoje te pamundur teknikisht per ta parandaluar dhe per ta raportuar si incident sigurie. Gjithashtu, ne kuptimin e Ligjit 9918/2008, neni 122 dhe Rregullores per Autorizimin e Pergjithshem, dergimi permes internetit nga pale te treta pa lidhje me operatorin e komunikimeve elektronike. i mesazheve SPAM qe mund te permbajne malware. nuk perben shkelje te detyrimeve per ruajtjen dhe garantimin e sigurise se perdoruesve nga ana e operatorit.
Per me teper, sa i perket e njoftimeve per software te demshem qe mund te shperndahen permes internetit (p.sh. pas marrjes dijeni si rezultat i ankesave te perdoruesve), ne kontekstin e qellimit te draft-ligjit "Per administrimin e sigurise kibernetike", monitorimi dhe raportimi i ketyre "software te demshem" vendoset nen kompetencen e ALCIRT, i cili do te jete sipas ketij Ligji organi pergjegjes per menaxhimin e procesit te administrimit te sigurise kibernetike ne bashkepunim me Keshillim e Sigurise Kibernetike dhe operatoret e infrastrukturave kritike te informacionit.
Persa me siper, sugjerojme qe SPAM te hiqet nga kategoria e software te demshem, dhe kategoria software te demshem te specifikohet si vijon:Software te demshem (virus, spyware, etj.) te cilet dergohen e jane nen kontrollin e drejtperdrejte te operatorit te komunikimeve elektronike."

Qëndrimi i AKEP:
AKEP merr ne konsiderate sygjerimi i ardhur, duke hequr SPAM nga kategoria e software te demshem.

Ne nenin 6 pika 5 e tij; mbrojtja e mjedisit te ciles i referohet AKEP gjykojme se eshte e paqarte si perkufizim dhe mbi te gjitha jashte kontekstit te Rregullores dhe objektit te saj. Mbrojtja e mjedisit rregullohet ne menyre te vecante me kuader specifik dhe te profilizuar, ndaj sugjerojme qe reference ne rregullore duhet te hiqet.

Qëndrimi i AKEP:
AKEP merr ne konsiderate propozimin e A dhe pika 5 e nenit 6 hiqet nga rregullorja.

Pika 13 e nenit 6 te Rregullores lidhur me informimin e perdoruesve per nje rrezik te vecante le vend per nje interpretim te gjere nga operatoret. Per kete, propozojme qe kushtet apo karakteristikat qe duhet te kete rreziku ne menyre qe te cmohet per nderhyrjen e operatorit sic percaktohet ne kete pike te Rregullores, te percaktohet qarte ne menyre qe te evitohen keqinterpretimet dhe kjo pike e rregullores te jete e zbatueshme ne menyre efikase.

Qëndrimi i AKEP:
AKEP sqaron se rrezik i vecante eshte cdo rrezik i cili kategorizohet si incident me impakt te larte ose te mesem, i cili afakton nje numer te konsdirueshem pajtimtaresh apo perben potencial per te afektuar.

Lidhur me piken 14 te nenit 6 te Rregullores, duke qene se eshte e ngjashme me percaktimet ne nenin 122 (pika 4) e Ligjit 9918/2008, kerkojme te sqarohet nga AKEP ne kete Rregullore se njoftimi ne AKEP do te kryhet ne rastet kur cenimi i te dhenave personale dhe shkeljeve te te dhenave personale eshte vene re nga vete operatori dhe jo nese operatori ka marre dijeni per shkeljen permes nje ankese te iniciuar nga vete perdoruesi per cenimin apo shkeljen e te dhenave te tij personale. Ne kete te fundit kompetenca me ligj i takon Komisionerit per te Drejten e Informimit dhe Mbrojtjen e te Dhenave Personale" ne perputhje me percaktimet e Ligjit 9887/2008 "Per Mbrojtjen e te dhenave personale".

Qëndrimi i AKEP:
AKEP sqaron se i permbahet perckaktimit te gjendur ne rregullore pasi kjo eshte nje detyrim qe rrjedh nga Ligji 9918, neni 122, pika 4.

Lidhur me piken 19 te nenit 6 te Rregullores, me qellim qartesimin e terminologjise se perdorur, A propozon qe pjesa e fjalise "Operatoret qe kryejne transaksione financiare online te zevendesohet me" Operatoret qe ofrojne vete apo permes te treteve transaksione financiare online".

Qëndrimi i AKEP:

AKEP merr ne konsiderate propozimin e ardhur nga operatori A.

Sipërmarrësi B

Pika (1),Operatorët duhet të informojnë AKEP brenda 3 ditëve, për secilin prej incidenteve të sigurisë. Komenti i B : Per Piken (1), si me siper, eshte i papercaktuar afati qe kane Operatoret per te njoftuar Akep, ky afat do të jetë për 3 ditë kalendarike apo për 3 ditë pune?

Qëndrimi i AKEP:
AKEP sqaron se behet fjale per 3 dite pune.

Pika (2), Operatorët duhet të informojnë AKEP menjëherë rreth incidenteve të zbuluara të sigurisë dhe/ose Cenimit të Integritetit, të cilat kanë pasur, kanë ose mendohet se do të kenë një impakt të rëndësishëm dhe / ose mesatar në ofrimin e rrjeteve të komunikimit publik dhe/ose në shërbimet e komunikimit elektronik publik të përdoruesit.

Komenti i B: Per Piken (2), si me siper,nuk percaktohet afati kohor.

Qëndrimi i AKEP:
Termi "menjehere" i referohet kohes se nevojshme, pa vonesa, qe i duhet operatorit per te pergatitur njoftimin i cili dergohet ne AKEP, por jo vone se 24 ore nga evidentimi i incidentit. Neni 6 pika 2 ndryshon dhe behet si me poshte vijon:

> ***"****Operatoret duhet te informojne AKEP rreth incidenteve te zbuluara te sigurise dhe/ose Cenimit te Integritetit, te cilat kane pasur, kane ose mendohet se do te kene nje impakt te rendesishem dhe / ose mesatar ne ofrimin e rrjeteve te komunikimit publik dhe/ose ne sherbimet e komunikimit elektronik publik te perdoruesit jo me vone se 24 ore nga evidentimi i incidentit.****"***

Pika (3) Operatorët duhet të implementojnë mjetet dhe metodat e duhura teknike dhe organizative për të garantuar sigurinë e rrjeteve të komunikimit publik dhe të shërbimeve të ofruara prej tyre. Këto mjete duhet të sigurojnë nivelin e sigurisë në përputhje me rrezikun e paraqitur dhe të evitojnë incidentet e sigurisë nga ndodhja e tyre ose të reduktojnë impaktin ose pasojat kur këto incidente ndodhin.

Komenti i B : Implementimet dhe rifreskimi i konfigurimeve të këtyre masave kërkon kohë, buxhet dhe burimet të tjera, ky proces është rekursiv dhe mund të ketë dhe probleme teknike gjatë procesit. Në këtë pikë AKEP mund të percaktojë kohën që duhet të kenë Operatorët për të implementuar këto kërkesa.

Qëndrimi i AKEP:
AKEP ben me dije se koha per marrjen e ketyre masave dhe implementimi i mjeteve, eshte percaktuar ne nenin 13 "Dispozita Kalimtare". Afati eshte 12 muaj nga hyrja ne fuqi te kesaj rregullore.

Pika (4) Operatorët duhet te implementojne mjetet e duhura teknike dhe organizative per te garantuar integritetin e rrjeteve te komunikimit publik, duke siguruar në këtë mënyrë ofrimin e pandërprerë të shërbimeve të tyre.

Komenti i B : Implementimet dhe rifreskimi i konfigurimeve të këtyre masave kërkon kohë, buxhet dhe burimet të tjera, ky proces është rekursiv dhe mund të ketë dhe probleme teknike gjatë procesit. Në këtë pikë AKEP mund të percaktojë kohën që duhet të kenë Operatorët për të implementuar këto kërkesa.

Qëndrimi i AKEP:
AKEP ben me dije se koha per marrjen e ketyre masave dhe implementimi i mjeteve, eshte percaktuar ne nenin 13 "Dispozita Kalimtare". Afati maksimal eshte 12 muaj nga hyrja ne fuqi te kesaj rregullore.

Pika (14) Në rast të cenimit të të dhënave personale, sipërmarrësi që ofron shërbime të komunikimeve elektronike të vlefshme për publikun njofton pa vonesë AKEP-in për këtë shkelje.

Komenti i B : Per piken (14), si me siper, nuk percaktohet afati kohor.

Qëndrimi i AKEP:
Termi "pa vonese" i referohet kohes fizike se nevojshme, qe i duhet operatorit per te pergatitur njoftimin i cili dergohet ne AKEP por jo me vone se 24 ore nga evidentimi i incidentit.
Neni perkates ndryshon si me poshte vijon:

> *"Në rast të cenimit të të dhënave personale, sipërmarrësi që ofron shërbime të komunikimeve elektronike të vlefshme për publikun njofton AKEP për këtë shkelje jo me vone se 24 ore nga evidentimi i saj."*

Pika (15) Kur një shkelje e të dhënave personale mund të ndikojë në privatësinë e pajtimtarit ose individit, sipërmarrësi, gjithashtu, njofton pa vonesë pajtimtarin ose individin për shkeljen.

Komenti i B : Per piken (15), si me siper, nuk percaktohet afati kohor.

Qëndrimi i AKEP:
Termi "pa vonese" i referohet kohes fizike se nevojshme, qe i duhet operatorit per te pergatitur njoftimin i cili dergohet pajtimtarit por jo me vone se 24 ore nga evidentimi i incidentit.
Neni perkates ndryshon si me poshte vijon:

> *"Kur një shkelje e të dhënave personale mund të ndikojë në privatësinë e pajtimtarit ose individit, sipërmarrësi, gjithashtu, njofton pajtimtarin ose individin për shkeljen jo me vone se 24 ore nga evidentimi i shkeljes"*

Pika 1 që shpreh detyrimin e referimeve në AKEP duhet t'i referohet edhe pikës dy për të specifikuar nivelin e rëndësisë së incidenteve që raportohen. Brenda tre ditëve, apo menjëherë dhe për cilat incidente? Afati kohor i raportimeve duhet te jetë i qartë në ditë kalendarike/pune.

Qëndrimi i AKEP:
Afati kohor i raportimit eshte 3 (tre) dite pune.

Pika 3 - Kush e bën vlerësimin e rrezikut të paraqitur?

Qëndrimi i AKEP:
Vleresimi i rezikut te paraqitur behet nga sipermarresi sipas rregullave te percaktuara ne legjislacionin ne fuqi.

Pika 7a. Qëllimet e përdorimit janë jo vetëm ligjore por kryesisht biznesi dhe me pas edhe ligjore, në të dyja rastet vetëm bazuar në legjislacionin përkatës.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate. Eshte ndryshimi perkates si me poshte vijon:

a) të sigurojnë që të dhënat personale të jenë të aksesueshme vetëm nga personeli i autorizuar bazuar në legjislacionin përkatës

Pika 8. Publikimi i referohet publikimit brenda kompanisë dhe palëve të treta të autorizuara?

Qëndrimi i AKEP:
Publikimi i rregullave per sigurine i referohet publikimit brenda kompanisë dhe palëve të treta të autorizuara.

Pika 11. Termi manual duhet të zëvendësohet me “udhëzime” dhe të specifikohet më qartë termi “ incidente të zakonshme të sigurisë” p.sh., në lidhje me të dhënat personale, në lidhje me viruse, etj.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate.Termi “ incidente me të zakonshme të sigurisë” u referohet incidenteve te cilat ndodhin me shpesh dhe ne menyre te perseritur.

Sipërmarrësi B kerkon qe neni 6 te riformulohet si me poshte:
2. Operatoret duhet te informojne AKEP menjehere rreth shkalles incidenteve te zbuluara te sigurise dhe/ose Cenimit te Integritetit, te cilat kane pasur, kane ose mendohet se do te kene nje impakt te rendesishem dhe / ose mesatar ne ofrimin e rrjeteve te komunikimit publik dhe/ose ne sherbimet e komunikimit elektronik publik te perdoruesit.

Qëndrimi i AKEP:
Operatoret duhet te informojme AKEP rreth incidenteve te zbuluara dhe rreth shkalles se kategorizimit te incidentit.

3. Operatoret duhet te implementojne zgjidhje teknike,masat e duhura teknike dhe organizative dhe metodat e kontrolleve të brendshme për të garantuar sigurinë e rrjeteve të komunikimeve publike dhe shërbimeve të ofruara prej tyre.
Keto mjete duhet te sigurojne nivelin e sigurise ne perputhje me rrezikun e paraqitur dhe te evitojne incidentet e sigurise nga ndodhja e tyre ose te reduktojne impaktin ose pasojat kur keto incidente ndodhin.

Qëndrimi i AKEP:
AKEP i qendron percaktimit dhe formulimit te nenit 6 pika 3 te rregullores.

7. Operatoret duhet të sigurojnë një nivel të mbrojtjes dhe sigurisë së përshtatshme ndaj rreziqeve të mundshme, të parashikuara. Masat qe operatoret do te ndermarrin duhet që, të paktën:
a) të sigurojnë që të dhënat personale të jenë të aksesueshme vetëm nga personeli i autorizuar për te suportuar ne sherbimet qe ofrojne ;
b) të mbrojnë të dhënat personale të ruajtura ose të transmetuara nga aksidentet apo nga shkatërrimi i kundërligjshëm, humbja ose ndryshimi aksidental dhe ruajtja, përpunimi, aksesi apo zbulimi i paautorizuar ose i jashtëligjshëm;
c) të sigurojnë implementimin e politikave të sigurisë, lidhur me përpunimin e të dhënave personale.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate pjeserisht. Verehet se jane paraqitur komente me qendrime te ndryshme per neni 6, pika 7.

12. Operatoret duhet te informojne perdoruesit e sherbimeve te rrjeteve te komunikimit publik ne lidhje me punet e planifikuara per mirembajtjen ose perditesimet, të paktën 1 dite përpara fillimit të punimeve te cilat mund te kene ndikim të lart dhe kohëzgjatja per mirëmbajtjen tejkalojnë SLA qe kane me palet e tyre te kontraktuara per dhënien e ketyre shërbimeve.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate pjeserisht. Pika perkatese ndryshon dhe behet si me poshte:

"Operatoret duhet te informojne perdoruesit e sherbimeve te rrjeteve te komunikimit publik ne lidhje me punet e planifikuara per mirembajtjen ose perditesimet, të paktën 1 dite përpara fillimit të punimeve te cilat mund te cilat mund te kene ndikim të lart dhe te sjellin nderprerje provizore te sherbimeve."

13. Operatoret duhet të informojnë përdoruesit e tyre për një rrezik të veçantë te lartë, mënyrën se si rreziku mund të reduktohet nga përdoruesit, si dhe kostot e mundshme, që duhet të mbulohen nga përdoruesi, nëse rreziku që ndodh është jashtë masave, që mund të marrë sipërmarrësi.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate.

Neni 7

Sipërmarrësi A

Ne nenin 7 nevojitet nje rinumertim per shkak te lapsuseve te formatimit ne tekst.

A vlereson se qellimi ne piken 7 te nenit 7 AKEP eshte njoftimi i perdoruesve te rrjeteve dhe sherbimeve te diet jane prekur nga incidenti i sigurise i vleresuar i larte. Me qellim qartesine dhe evitimin e keqinterpretimeve, propozojme qe kjo pike te riformulohet si vijon: "Njofton perdoruesit e rrjeteve dhe/ose sherbimeve te prekur, rreth incidentit te sigurise, ne rast se e konsideron e larte impaktit e incidentit te sigurise."

Qëndrimi i AKEP : *Eshte marre parasysh komenti i A ne lidhje me saktesimin e kesaj pike ne nenin 7. Neni perkates ndryshon si me poshte vijon:*

"Njofton perdoruesit e rrjeteve dhe/ose sherbimeve te prekur, rreth incidentit te sigurise, në rast se e konsideron si te larte impaktin e incidentit te sigurise."

Sipërmarrësi B

Ne Nenin (7), Pika (3) dhe (4) mungojnë.

Pika (7) AKEP Njofton përdoruesit e rrjeteve dhe/ose shërbimeve rreth incidentit të sigurisë, në rast se e konsideron si të lartë impaktin e incidentit të sigurisë.

Komenti i B: Nuk eshte e qarte situata nese operatorët do të njoftohen në këtë rast?
Duke pasur parasysh qe një proces i tillë mund të ketë impakt negativ në biznes për operatorin AKEP duhet te njoftoje edhe operatoret.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e ardhur nga B . Neni perkates ndryshon si me poshte vijon:

"Njofton perdoruesit e rrjeteve dhe/ose sherbimeve te prekur, rreth incidentit te sigurise, në rast se e konsideron si te larte impaktin e incidentit te sigurise duke vene ne dijeni operatorin e rrjetit ose sherbimit perkates."

Pika (8) Kryen kontrolle në mënyrë periodike në bashkëpunim me ALCIRT, për të verifikuar implemetimin e kësaj rregulloreje.

Komenti i B : Eshte e papërcaktuar koha kur Operatorët do të njoftohen për këto audite. Perderisa citohet se do te jene kontrolle periodike duhet te percaktohet peridoiciteti i tyre nese do te jene 6 mujore apo vjetore etj.

Në këto kërkesa duhet të përcaktohen sistemet të cilat do të jenë subjekt i këtij auditi si dhe formati standart i auditimit i cili te jete si aneks i kesaj rregulloreje.

Audituesit duhet të kenë një program të veçantë pune i cili te bazohet ne formatin standart dhe duhet të rishikohet nga Operatori.

Pika 6. Nuk është e qartë mënyra e investigimit të AKEP: në bashkëpunim me operatorët? Në këtë rast këta të fundit duhet të llogarisin edhe pjesën e nevojshme të personelit; nëse është në mënyrë të pavarur, konkluzionet duhet të jenë transparente edhe për operatorët.

Sipërmarrësi B kerkon qe neni 7 te riformulohet si me poshte:
9. Ndermerr masat taknike sipas legjislacionit në fuqi nese operatoret nuk plotesojne kërkesat dhe kushtet e kesaj rregulloreje.

Qëndrimi i AKEP:
AKEP merr ne konsiderate pjeserisht komentin e B duke saktesuar ne rregullore rastet kur mund te behen kontrollet. Neni perkates ndryshon si me poshte vijon:

> *"Kryen kontrolle ne bashkepunim me ALCIRT, per te verifikuar implemetimin e kesaj rregulloreje ne rastet kur shihet e nevojshme."*

Pika (9) Ndërmerr masa sipas legjislacionit në fuqi nëse operatorët nuk plotësojnë kërkesat dhe kushtet e kësaj rregulloreje.

Komenti i B: Formulimi ne piken (9), si me siper, per marrjen e masave sipas legjislacioni ne fuqi nese operatoret nuk plotesojne kerkesat dhe kushtet e kesaj rregullore eshte evaziv dhe le hapesire te gjere per interpretime.

Te percaktohet ne rregullore se cilat jane masat qe ndermerr rregullatori ne raste te tilla. Per me teper duhet percaktuar edhe intervali kohor ku Operatorit i lihet kohë për t'i mbyllur/korrigjuar problematikat e evidentuara nga auditoret.

Qëndrimi i AKEP:
AKEP ne pergjigje te komentit te B ben me dije se masat qe mund te marre AKEP jane te percaktuar ne ligjin nr.9918. Persa i perket intervalit kohor operatoret kane 12 muaj kohe, bazuar ne nenin 13 per te bere auditin e sistemeve te tyre dhe per te korrigjuar problemet nese indentifikohen.

Neni 8

Sipërmarrësi B

Pika 6. Operatorët kanë nevojë që të dhënat t'i aksesojnë edhe **në" kuadër të përmirësimit të shërbimeve"**, jo vetëm për ofrimin.

Sipërmarrësi B kerkon qe neni 8 te riformulohet si me poshte:
4. Operatoret, personat e autorizuar, punonjesit, dhe cdo individ i përfshirë në sistemet e komunikimeve elektronike, pjesë e strukturave të Operatorit jane pergjegjes per ruajtjen e te dhenave dhe mbrojtjen e konfidencialitetit te te dhenave dhe komunikimeve dhe periudhes se ruajtes se te dhena te percaktuar prej rregullatorit.

Qëndrimi i AKEP:
AKEP i qendron percaktimit ne nenin 8 pika 6.

Neni 9

Sipërmarrësi A

Lidhur me vleresimin e impaktit te incidenteve te sigurise, A eshte dakord me ndarjen ne incident te ulet te mesem e te larte. si dhe me rekomandimin per te njoftuar AKEP vetem per incidentet e vleresuara te mesme e te larta.
Sa i perket kritereve te klasifikimit/vleresimit te incidenteve te sigurise, kombinimit te tyre, ne kuptim te objektit dhe qellimit te Rregullores, i cili lidhet ngushte me sherbimet dhe rrjetet te cilat ofrojne sherbime dhe kane te dhena personale te perdoruesve, A vlereson se kriteri primar i cili duhet te klasifikoje nje incident nese eshte I ulet, 1 mesem apo i larte eshte numri i pajtimtareve te prekur, e kombinuar me kohezgjatjen e incidentit dhe vetem ne rastet kur numri i pajtimtareve eshte i panjohur incidenti mund te vleresohet nga shtrirja gjeografike per rastet e mohimit te sherbimit.
Ne kete kontekst, duke marre parasysh standardet nderkombetare, propozojme si vijon:

Pika 3 e Nenit 9 te ndryshohet si vijon:
a. "Incidentet e sigurise konsiderohen si incidente me impakt te larte nese numri i perdoruesve te ndikuar nga incidenti eshte minimalisht sa 5% e numrit total te perdoruesve, por jo me pak se 1000 perdorues."
b. "Incidentet e sigurise konsiderohen si incidente me impakt te ulet nese numri i perdoruesve te ndikuar nga incidenti eshte minimalisht sa 0.2% e numrit total te perdoruesve. por jo me shume se 1000."
Sa me siper e propozojme me qellim vleresimin analog e te drejte te incidentit per cdo operator pavaresisht numrit total te pajtimtareve te tij.

Qëndrimi i AKEP:
AKEP merr ne konsiderate pjeserisht komentit e A,duke reflektuar perkufizimin ne lidhje me incidentin e sigurise me impakt te ulet ne lidhje me numrin e pajtimtareve ne piken 2 te nenit 9.

Pika 4 e Nenit 9 te ndryshohet si vijon: "Ne rast se numri i pajtimtareve eshte i panjohur, incidentet e sigurise do te konsiderohen si incidente me impakt te larte nese zona gjeografike e shtrirjes se tij eshte minimalisht 10 km, per rastet kur incidenti eshte shkaktuar si pasoje e mohimit te sherbimit."

Qëndrimi i AKEP:
AKEP ne rastin e pikes 4 te nenit 9 ben me dije se kriter vleresim eshte shtrirja e incidentit bazuar ne zone gjeografike.

Sipërmarrësi C

Lidhur nenin 9/2, “Incidentet e sigurise qe kane pasur kohezgjatje me pak se 1 ore, ne menyre automatike konsiderohen si te nje impakti te ulet dhe nuk eshte i nevojshem plotesimi i tabeles", C kerkon modifikimin e ketij neni/pike si me poshte;

Neni 9/2
"Incidentet e sigurise qe kane pasur kohezgjatje me pak se 1(nje) ore me pak se 2 (dy) ore, ne menyre automatike konsiderohen si te nje impakti te ulet dhe nuk eshte i nevojshem plotesimi i tabeles"

Qëndrimi i AKEP:
AKEP i qendron percaktimit ne rregullore duke e mbajtur afatin kohor maksimal ne 1 (nje) ore

Persa i perket nenit 9/3, "Incidentet e sigurise konsiderohen si incidente me impakt te larte nese numri i perdoruesve te ndikuar nga incidenti ose perqindja e tyre ndaj perdoruesve total eshte minimalisht 1000 ose 5%. C kerkon qe ky nen/pike te ndryshohet/modifikohet sime poshte;

Neni 9/3;
"Incidentet e sigurise konsiderohen si incidente me impakt te larte nese numri i perdoruesve te ndikuar nga incidenti ose perqindja e tyre (%) ndaj perdoruesve total eshte minimalisht 1000 ose mbi 10% e abonenteve te te gjithe kategorive te sherbimit.

Qëndrimi i AKEP:
AKEP i qendron percaktimit ne rregullore duke e mbajtur limitin e perqindjes te abonenteve ne 5%, pasi vlereson se kjo perqindje eshte nje vlere e konsiderueshme e bazes se pajtimtareve.

Po ashtu, ne nenin 9/4, ku percaktohet se;"Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtritjes se tij eshte minimalisht 10 km, C argumenton qe;
Impakti qe sjell nje incident sigurie i cili ndodh ne nje lokalitet ku gjenden qendrat me te rendesishme te funksionimit te shtetit dhe per me teper me perqendrim te larte abonentesh, nuk eshte i njejte me impaktin qe do te sillte ndodhja e nje incidenti ne zona/rajone apo lokalitete ku keta faktore jane me pak prezent. Per kete arsye C kerkon ndryshimin/modifikimin e ketij neni/pike si me poshte;

Neni 9/4;
'Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtritjes se tij eshte me shume se 10 km per rrjetin fix, 10 km per rrjetin mobile ne qytetin e Tiranes, si dhe 60 km per zona te tjera te Shqiperise".

Qëndrimi i AKEP:
AKEP vlereson komentin e C duke e marre ne konsiderate pjeserisht. Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtritjes se tij eshte minimalisht 20 km^2.

Sipërmarrësi B

Komenti i B: Formula e përllogaritjes së impaktit është jo shumë e qartë dhe në disa raste jo e saktë.

Nëse do të ketë raste të veçanta të Incidenteve të Sigurisë së Informacionit (p.sh., incidentet e Interceptimit) edhe intervale më të shkurtra kohore se 1 orë prej B konsiderohen incidente të një impakti tepër të lartë pasi në këtë rast janë thyer të gjitha mekanizmat e sigurisë së rrjetit të komunikimit.

Ne tabelën e Aneksit 2, limiti i sipërm për ndërprerjet mund të zgjerohet me teper se 4 orë.

Afati kohor prej 15 ditësh nuk është i mjaftueshëm në disa raste për të nxjerrë një vlerë të saktë të impaktit. Nëse konsiderojmë që disa prej sistemeve tona janë të hostuara jashtë Shqipërisë ky proces mund të marrë më shumë se 15 ditë, pasi vlerësimi do të kalojë në disa grupe vlerësimi dhe më pas në B për vlerësimin final.

Qëndrimi i AKEP:

AKEP vlereson komentin e B duke marre ne konsiderate pjeserisht.
Limiti kohor per vleresimin perfundimtar behet 30 dite. Ne lidhje me limitin kohor ne Aneks 2 AKEP vlereson se limit kohor prej dy oresh duhet te qendroj dhe jo te zgjatet ne 4 ore, pasi edhe dy ore eshte nje interval kohor i konsiderueshem.

Pika 2, 3, dhe 4. Klasifikimi i incidenteve të sigurisë duke marrë parasysh vetëm kohëzgjatjen, apo shtrirjen fizike mund të çojë në klasifikim jo të saktë; kohëzgjatja duhet të jetë si referente për impaktin e incidentit kur ky i fundit rezulton në ndërprerje të shërbimeve; vlerësimi i kritikalitetit duhet të jetë një metodologji që kombinon tregues të tipit të të dhënave që impaktohet, nr të klienteve, kohëzgjatjen dhe **kohën e nevojshme për t'u kthyer në gjendjen e mëparshme.**

Qëndrimi i AKEP:
Per te klasifikuar nje incident si incident me impakt te larte mjafton qe njeri nga parametrat e percaktuar (kohezgjatja, numri i pajtimtareve dhe shtrirja gjeografike) te permbushet.

Pika 6. Përcakton vetëm incidentin madhor. Nuk qartësohet kush është një incident mesatar.

Qëndrimi i AKEP:
Incident mesatar klasifikohet cdo incident i cili kalon limitet e percaktuara per nje incident te ulet por gjithashtu parametrat nuk arrijne ne limitet per tu klasifikuar sin je incident me impakt te larte.

Po rasti nëse një parametër është i lartë dhe parametri tjetër është i ulët? Metodologjia e vlerësimit të impaktit duhet të varet nga tipi i incidentit.

P.sh., një interceptim i paautorizuar është më vete një incident serioz pavarësisht nga kohëzgjatja ose nr i personave të ndikuar; gjithashtu vlerësimi i një programi/software të dëmshëm nuk mund vlerësohet në bazë të orëve ose të hapësirës gjeografike.

Në fakt, meqë të gjithë operatorët kanë metoda të bazuara në rregullore/standarte ndërkombëtare për klasifikim dhe reagimin ndaj incidenteve, do ishte mirë që AKEP të merrte parasysh këto metodologji për të standartizuar edhe mënyrën e raportimit. Mungesa e këtij standartizimi do ketë dy efekte:

1. Përpjekje ekstra dhe kosto për operatorët për të mbajtur dy mënyra raportimi dhe reagimi;
2. Gabime në raportim dhe klasifikime të ndryshme nga operatorë të ndryshëm që mund të shkaktojnë kosto ekstra dhe mungesë të saktë informacioni në lidhje me risqet e rëndësishme të tregut.

Qëndrimi i AKEP:
Per te klasifikuar nje incident si incident me impakt te larte mjafton qe njeri nga parametrat e percaktuar (kohezgjatja, numri i pajtimtareve dhe shtrirja gjeografike) te permbushet.

Pika 8. Mund të ndodhë që incidenti i sigurisë të kërkojë më shumë kohë për investigim;

Qëndrimi i AKEP:
Eshte marre ne konsiderate propozimi i operatorit B duke e rritur kohen e nevojshme per investigim nga 15 ne 30 dite.

B Albania kerkon qe neni 9 te riformulohet si me poshte:

1. Operatoret duhet te kryjne vleresimin periodik te impaktit te incidenteve te sigurise sipas tabeles se paraqitur ne Aneksin 2.

Qëndrimi i AKEP:
AKEP cmon se vleresimi i impaktit duhet te jete referuar pas ndodhjes se cdo incidenti dhe jo ne menyre periodike.

2. Incidentet e sigurise qe kane pasur kohezgjatje me pak se 1 ore, ne menyre automatike konsiderohen si te nje impakti te ulet dhe nuk eshte i nevojshem plotesimi i tabeles.

Qëndrimi i AKEP:
Operatori B eshte i te njejtit qendrim me percaktimin ne rregullore te AKEP.

3. Incidentet e sigurise konsiderohen si incidente me impakt te mesatar nese numri i perdoruesve te ndikuar nga incidenti ose perqindja e tyre (%) ndaj perdoruesve total eshte minimalisht 1000 ose 5%.

Qëndrimi i AKEP:
AKEP i qendron percaktimit se incidenti me numer te perdoruesve total minimalisht 1000 ose 5% e totalit klasifikohet si incident me impakt te larte.

4. Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtrirjes se tij eshte minimalisht 10 km² ose perqindja eshte me teper se 5%.

Qëndrimi i AKEP:
Operatori B eshte i te njejtit qendrim me percaktimin ne rregullore te AKEP.

5. Ne cdo rast tjeter, incidentet e sigurise konsiderohen si incidente me impakt mesatar.

Qëndrimi i AKEP:
Operatori B eshte i te njejtit qendrim me percaktimin ne rregullore te AKEP.

Neni 10

Sipërmarrësi A

Ne nenin 10 pika 2 e Rregullore, lidhur me kerkesen per kryerjen e auditit te sigurise nga nje organ I certifikuar dhe i pavarur, ose nga autoriteti kompetent nje here ne 2 vjet per subjektet me te ardhura vjetore te vitit paraardhes mbi vleren 100,000,000 leke, A vlereson se ne kete pike mbetet e paqarte se cili do te jete objekti i auditit te sigurise. i cili do te konsiderohet nga AKEP i vlefshem per qellimet e kesaj Rregulloreje, cilet organe kuailfikohen si organe te certifikuara te pavaruar qe mund te kryejne auditin e sigurise sipas kesaj Rregulloreje, si dhe kush eshte autoriteti kompetent te cilit i ben reference neni perkates, cka kerkojme te sqarohen duke riformuluar nenin perkates.

Konkretisht ne kuader te auditimit te pervitshem financiar nga auditoret tane te jashtem (PWC aktualisht), A auditohet edhe sa i perket masave te sigurise per disa nga sistemet kritike te informacionit A sugjeron qe edhe auditoret financiare te jashtem si PWC te konsiderohen organe te certifikuara e te pavaruara, si dhe auditimi Lidhur me sigurine i kryer prej tyre te konsiderohet auditim i mjaftueshem sigurie nga AKEP per nevojat e kesaj Rregulloreje.

Gjithashtu, duke qene se procesi i auditimit te jashtem nder te tjera eshte i kushtueshem dhe kerkon alokimin e burimeve njerezore dhe financiare te nevojshme, A sugjeron qe auditimi i sigurise te kryhet ne menyre periodike nga vete AKEP, i cili eshte organi mbikqyres pergjegjes per zbatimin e kerkesave te Ligjit 9918/2008, Autorizimit te pergjithshem dhe rregulloreve perkatese lidhur me masat e sigurise se rrjeteve e sherbimeve te ofruara nga operatoret e komunikimeve elektronike.

Qëndrimi i AKEP:

AKEP vlereson komentin e A dhe sqaron se objekti i auditit te sigurise do te jete i njejte me objektin dhe procedurat e percatuara ne Aneks 3, bashkelidhur kesaj rregullore. Ne lidhje me auditin e certifikuar e pavarur AKEP ben me dije se eshte ne vullnetin e kompanise te zgjedhe auditin, i cili te jete i pavarur nga operatori, por duke plotesuar kushtet qe te jete i certifikuar per ISMS (Information Security Managment Systems). Ne lidhje me kryerjen e auditit nga vete AKEP, ju bejme me dije se ne AKEP do te kryehet vetem depozitimi i rezultateve te auditit ne rastin e operatoreve te me te ardhura vjetore mbi 100.000.000 leke.

Sipërmarrësi C

Nderkohe, C vlereson si tejet te rendesishme percaktimet e nenit 10 te draft Rregullores
mbi raportimin e masave te sigurise dhe auditit. Ne kete nen eshte percaktuar nje kategorizim i sipermarresve bazuar ne raportimin vjetor te te ardhurave te ketyre te fundit,sipas te cilit vlera prej 100.000.000 lek sherben si vlera varesisht te ciles sipermarresi eshte subjekt i detyrimit per raportimin ne forme vet-deklarimi mbi masat e sigurise ose te dorezoje prane AKEP raportin me rezultatet e auditit te sigurise.

Formulimi ne teresi i nenit 10, vjen ne kundershtim me percaktimet e nenit 7, pika 3/e) e Ligjit nr. 9918 dt. 19.05.2008, i ndryshuar Komunikimet Elektronike ne Republiken e Shqiperise" sipas te cilit AKEP nxit konkurencen eficente per sigurimin e rrjeteve dhe te sherbimeve te komunikimeve elektronike per te siguruar mosdiskriminimin dhe barazine ne trajtimin e ofruesve te rrjeteve dhe sherbimeve. Keshtu, te gjithe sipermarresit duhet te jene subjekt i detyrimeve me natyre te njejte per sa kohe qe po keta sipermarres pergjigjen po ne menyre te njejte perballe AKEP dhe perballe detyrimeve te percaktuara nga Ligji, kryejne pagesat sipas percaktimeve te Ligjit sipas vlerave te percaktuara ne aktet ligjore njesoj per te gjithe sipermarresit etj. Ndaj, dhe ne kete kuptim, nuk mundet qe nje kategori e caktuar sipermarresish te trajtohet ne menyre diskriminuese favorizuese dhe nje pjese tjeter te rendohet me nje kosto tejet te larte financiare.

Pavaresisht madhesise se rrjetit apo nivelit te te ardhurave, siguria dhe integriteti i rrjeteve eshte po njesoj i rendesishem si per pajtimtarin e nje operatori te vogel ashtu edhe per pajtimtarin e nje operatori te madh. Madje, operatore te medhenj (praktikisht ata qe sipas kesaj draft rregulloreje kane te ardhura vjetore me shume se 100.000.000 leke) kane ne fakt rrjete dhe teknologji me te zhvilluar ku masat e sigurise dhe te integritetit te rrjetit i kane si nje ceshtje te rendesishme per interesin e vet kompanise, investimeve ne rrjet dhe cilesise se sherbimeve te ofruara, pertej cdo detyrimi te vendosur. Nderkohe qe, me se shumti ndeshet pikerisht tek keta sipermarres "te vegjel" mos permbushja e standarteve ne operimin e aktivitetit te ofrimit te rrjeteve dhe sherbimeve dhe mosplotesimi i kushteve dhe rregulloreve te AKEP ne lidhje me ndertimin dhe funksionimin e rrjeteve te komunikimeve elektronike. Ndaj dhe nese do te ishte e nevojshme, certifikimi me audit sigurie do te duhej pikerisht per keta sipermarres dhe jo per operatoret qe kane rrjete me shtrirje te gjere dhe teknologji te zhvilluar te cilet, ashtu sic referuam me lart, interesin per mbrojtjen e rrjeteve dhe sherbimeve e kane edhe kryesisht pavaresisht detyrimeve rregullatore .

Per me teper, neni 122, pika 10 e Ligjit i cili percakton mundesine per vendosjen e detyrimeve per vete-deklarimin mbi masat e sigurise apo paraqitjen e auditit te sigurise nuk parashikon mundesine per trajtimin e diferencuar te sipermarresve varesisht ndonje kriteri dhe akoma me shume, ky nen nuk percakton asnje kriter fmanciar te lidhur me te ardhurat e sipermarresit per kategorizimin e ketyre te fundit me qellim vendosjen e detyrimeve. Keshtu, ne percakimin e detyrimeve ndaj operatoreve dhe per me teper kur keto detyrime jane me kosto te larte financiare per sipermarresit, do duhej qe ne cdo

rast ky kriter te ishte i parashikuar qartesisht nga Ligji. Po ashtu, edhe percaktimi i vleres prej 100.000.000 lek krijon diskutime te shumta pasi ne kete rast brenda te njejtes kategori, sic mund te jete rasti i sipermarresve me te ardhura mbi 100.000.000 leke, ka sipermarres qe nga keto te ardhura kane fitime te konsiderueshme po ashtu ka sipermarres qe jo vetem nuk kane fitim por kane rezulutar me humbje duke bere teresisht te ndryshme pozicionin financiar te sipermarresve brenda se njejtes kategori. AKEP i disponon te gjitha te dhenat financiare te operatoreve ndaj dhe AKEP duhej te kishte konsideruar edhe kete fakt ne vendosjen e ketij kriteri ne draft rregullore.
Per sa parashtruam me lart, C kerkon qe neni 10 te rifromulohet ne teresi si me poshte;

Neni 10
Te gjithe sipermarresit e sherbimeve te komunikimeve elektronike duhet te raportojne ne AKEP ne formen e nje vetdeklarimi masat e marra te sigurise periodikisht nje here ne vit brenda muajit Janar per vitin paraardhes sipas Aneksit 3.

Ose ne meyre alternative;

Neni 10
Te gjithe sipermarresit e sherbimeve te komunikimeve elektronike duhet qe te dorezojne prane AKEP raportin me rezultatet e auditit te sigurise, te kryer nga nje organ i certifikuar dhe i pavarur ose nga autoriteti kompetent.
Raporti duhet te dorezohet periodikisht per nje periudhe jo me shume se dy vjecare. Kostoja e auditit do te paguhet nga sipermarresi.

Qëndrimi i AKEP:
AKEP bazuar ne madhesine e operatoreve dhe ne gamen e gjere te sistemeve dhe sherbimeve qe disponojne operatoret e grupuar ne piken 2 te nenit 10 vlereson se pervec vetedeklarimit, eshte i nevojshem dhe kryerja e auditit nga nje organ i specializuar.
Ne lidhje me operatoret te clet do te depozitojne vetem vetedeklarim sipas Aneks 3, AKEP ben me dije se gjate inspektimeve qe do te kryehen do te behet dhe verifikimi i raportimeve, ku do te vleresohet perputhshmeria ne lidhje me cfare eshte deklaruar dhe cfare eshte zbatohet konkretisht nga sipermarresi.

Persa i perket percaktimit ne nenin 10/7 te projekt-rregullores ku percaktohet se ;
"AKEP mund te kerkoje te dhena te tjera shtese, pervec atyre ne formularin perfundimtar, ne lidhje me incidentin e sigurise. Per kete arsye, operatoret jane te detyruar te ruajne te gjithe te dhenat ne lidhje me incidentet esigurise se raportuar per nje periudhe kohore prej 18 muaj qe nga koha e dorezimit te njoftimitperfundimtar rreth incidentit te sigurise.
C kerkon qe;
Afati kohor i ruajtjes se te dhenave duhet te jete me i shkurter se 18 muaj pasi akualisht C apo cdo operator tjeter, si pasoje e detyrimeve ligjore per qellime specifike detyrohet te ruaje te dhena per afate edhe me te gjata. Nje detyrim i ri sipas kesaj projekt-rregulloreje per te ruajtur edhe keto te dhena dhe me afate te tilla te gjata do te rendonte mbi proceset operative te kompanise si dhe ne kostot financiare per grumbullimin, ruajtjen/manaxhimin e ketyre te dhenave. Per kete arsye C kerkon qe ky nen/pike te ndryshohet/modifikohet si me poshte;

Neni 10/7;

AKEP mund te kerkoje te dhena te tjera shtese, pervec atyre ne formularin perfundimtar, ne lidhje me incidentin e sigurise. Per kete arsye, operatoret jane te detyruar te ruajne te gjithe te dhenat ne lidhje me incidentet e sigurise se raportuar per nje periudhe kohore prej 6 muajsh nga koha e dorezimit te njoftimit perfundimtar rreth incidentit te sigurise.

Qëndrimi i AKEP : *AKEP merr ne konsiderate komentin e C dhe jane pasqyruar ndryshimet perkatese ne nenin 10, pika 7 ku periudha kohore eshte bere 6 muaj.*

Sipërmarrësi B

Pika (2), Sipërmarrësit e komunikimeve elektronike që rezultojnë sipas raportimeve të kryera në AKEP me të ardhura vjetore te vitit paraardhës nga komunikimet elektronike mbi vlerën 100,000,000 lekë, duhet që të dorezojnë pranë AKEP raportin me rezultatet e auditit të sigurisë, të kryer nga një organ i çertifikuar dhe i pavarur ose nga autoriteti kompetent.

Raporti duhet të dorëzohet periodikisht për një periudhë jo më shumë se dy vjecare. Kostoja e auditit do të paguhet nga sipërmarrësi.

Komenti i B : Këto Audite kanë një kosto të lartë pasi bazohen në numrin e sistemeve, aplikimeve dhe pajisjeve që do të jenë në proces. Në disa raste mund të krijojnë dhe probleme me shërbimet e biznesit. AKEP mund të marrë në konsideratë që kjo periudhë kohe të jetë më e madhe.

Qëndrimi i AKEP:
AKEP vlereson se periudha 2 vjecare eshte kohe e mjaftueshme per te kryer nje audit sigurie.

Pika 2. Duhet përcaktuar qartë kush është organi i çertifikuar, ose autoriteti kompetent. Zakonisht këto audite bëhen nga trupa çertifikuese të cilat gjithashtu kërkojnë një audit të brendshëm paraprak. Për plotësimin e kësaj pike, duhet që operatorëve t'i lihet një kohë më e gjatë në dispozicion në mënyrë që të implementojnë kërkesat.

Qëndrimi i AKEP:
AKEP ben me dije se eshte ne vullnetin e kompanise te zgjedhe auditin e certifikuar i cili te jete i pavarur nga operatori, por duke plotesuar kushtet qe te jete i certifikuar edhe per ISMS (Information Security Managment Systems).

Neni 11

Sipërmarrësi A

Ne nenin 11 pika 1. A sugjeron qe ne fund te fjalise te shtohet pjesa, "....me kerkesen e AKEP', ne menyre qe sipermarresit te ofrojne informacion lidhur me politikat e dokumentuar ate sigurise me kerkesen e AKEP.

Qëndrimi i AKEP:
AKEP vlereson se komenti i A eshte i perfshire me kete pike te nenit.

Sa i perket nenit 11 pika 3. A vlereson se informacioni i shkembyer me AKEP lidhur me incidentet perben informacion konfidencial te operatorit e duhet trajtuar si i tille nga AKEP ne baze te Ligjit 9918/2008, neni 8 pika nje, neni 16 pika 5, e nuk duhet te publikohet pa pelqimin paraprak te sipermarresit. Per me teper, publikimi i informacionit lidhur me incidentet e sigurise vleresojme se eshte ne objektin e veprimtarise ligjore te ALCIRT, i cili eshte autoriteti pergjegjes qe ne bashkepunim me sipermarresit dhe ne baze te ligjit (ende draft) "Per administrimin e sigurise kibernetike", do te duhet te percaktoje kriteret dhe kushtet e qarta e transparente, qe duhet te permbushen ne menyre qe nje incident sigurie te behet publik. Bazuar ne sa me siper, per nevojat e kesaj Rregulloreje propozojme qe ne fund te paragrafit 3 te nenit 11 te shtohet:

" per sa kohe qe nuk cenon integritetin e rrjeteve te operatorit dhe nuk shperndan informacion konfidencial ose sekret biznesi"

Qëndrimi i AKEP:
AKEP duke respektuar parimet e konfidencialitetit i qendron pikes 3 te nenit 12 pasi eshte e bazuar ne ligjin nr.9918 datë 19.5.2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar, neni 122, pika 12:

> *"AKEP-i mund të informojë vetë publikun ose të kërkojë nga sipërmarrësi që ta njoftojë atë, nëse vlerëson që bërja publike e kësaj shkeljeje është në interes të publikut."*

Sipërmarrësi C

Se fundmi, persa i perket nenit 11, paragraf 3, ne te cilin prashikohet qe AKEP per arsye sigurie mund te njoftoje publikun rreth incidenteve te sigurise qe kane ndodhur ose qe mund te ndodhin, edhe pa marre pelqimin paraprak te operatorit;
C kerkon qe ne kete nen, ose te hiqet pjesa " edhe pa marre pelqimin paraprak te operatorit" dhe te behet "me pelqimin paraprak e operatorit" ose te garantohet kujdesi nga AKEP per mos cenimin e imazhit te operatorit nga publikime te tilla apo menyra e publikimit.

Qëndrimi i AKEP:

AKEP duke respektuar parimet e konfidencialitetit i qendron pikes 3 te nenit 12 pasi eshte e bazuar ne ligjin nr.9918 datë 19.5.2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar, neni 122, pika 12:

> *"AKEP-i mund të informojë vetë publikun ose të kërkojë nga sipërmarrësi që ta njoftojë atë, nëse vlerëson që bërja publike e kësaj shkeljeje është në interes të publikut."*

Sipërmarrësi B

Per arsye sigurie, AKEP duke patur Raportin e Vleresimit te Impaktit mund te njoftoje publikun rreth incidenteve te sigurise, qe kane ndodhur ose qe mund te ndodhin ne te ardhmen ne komunikimet elektronike publike edhe pa marre pelqimin paraprak te operatorit.
Komenti i B : AKEP mund të publikojë këtë raport mbasi të ketë marrë prej Operatorit Raportin e Vlerësimit së Impaktit.

#SO 11: Kontrolli i aksesit në rrjetin dhe sistemet e informacionit.

Komenti i B: Regjistrimet e hyrjeve/Logs që do të jenë qëllimi i proceseve duhet të jenë te lidhura vetëm me regjistrimet e të dhënave kritike.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e B. Pika 3 e nenit 12 behet si me poshte:
"Per arsye sigurie, AKEP mund te njoftoje publikun rreth incidenteve te sigurise, qe kane ndodhur pasi ka marre vleresimin e impaktit te incidentit te sigurise ose qe mund te ndodhin ne te ardhmen ne komunikimet elektronike publike edhe pa marre pelqimin paraprak te operatorit".

Sipërmarrësi B kerkon qe neni 11 te riformulohet si me poshte:

Investigimi i Incidenteve te Sigurise dhe Cenimit te Integritetit

Duke vleresuar nivelin e riskut te incidentit te sigurise dhe/ ose cenimit te integritetit te raportuar sipas Formularit ne aneksin 1, AKEP mund te ndermarre veprimet e nevojshme per investigimin e ketij incidenti te sigurise dhe po ashtu per sqarimin e te gjitha rrethanave percaktuar nga njoftimi i operatorit.

Qendrimi i AKEP:
Komenti i sipercituar eshte i njejte dhe ne perputhje me percaktimin e kesaj pike ne rregullore.

Nese eshte e nevojshme, ne kuader te investigimit, AKEP do te informoj Agjensine Kombetare te Sigurise Kompjuterike (ALCIRT) dhe organet e tjera konpetente ne perputhje me legjislacionin për transmetimin e te dhenave nderkombetare.

Qendrimi i AKEP:
Komenti i sipercituar eshte i njejte dhe ne perputhje me percaktimin e kesaj pike ne rregullore.

Per arsye sigurie, AKEP duke patur Raportin e Vleresimit te Impaktit mund te njoftoje publikun rreth incidenteve te sigurise, qe kane ndodhur ose qe mund te ndodhin ne te ardhmen ne komunikimet elektronike publike edhe pa marre pelqimin paraprak te operatorit.

Qendrimi i AKEP:
AKEP merr ne konsiderate komentin e ardhur nga operatori B, i cili eshte reflektuar ne piken 3 te nenit 11.

Neni 12

Sipërmarrësi A

Ne nenin 12 pika 1, referenca e nenit ne piken e pare nuk kane permbushur nje ose disa nga detyrime te nenit 5 duhet te jete neni 6.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e A.

Ne nenin 12 pika 3, sugjerojme qe te ndryshoje si vijon: "Kane bere qellimisht vleresim jo te vertete te impaktit te incidentit te sigurise duke menjanuar ne kete menyre detyrimin e raportimit sipas standardeve te sigurise ISO.

Qëndrimi i AKEP:
AKEP i qendron perckatimit te kesaj pike.

Neni 13

Nuk ka

Neni 14

Nuk ka

Aneksi 1

Sipërmarrësi A

Ne Aneksin 1 - seksioni Pershkrimi i incidentit te sigurise dhe/ose cenimit te integritetit tek pika "Zona gjeografike e prekur nga Incidenti i sigurise dhe/ose cenimi i integritetit" sugjerojme qe te percaktohet njesia e raportimit (p.sh. km^2).
Me tej lidhur me plotesimin e pikave "Burimet e prekura" dhe "Pasojat" kerkojme sqarim per menyren e plotesimit.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e A duke shtuar njesine km^2 ne piken perkatese. Ne lidhje me kerkesen per sqarim ben me dije se me "Burimet e Prekura" i referohet sistemeve dhe sherbimeve te operatorit te cilat jane prekur nga incidenti. Me "Pasojat" i referohet efekteve dhe demeve te cilat ka sjelle incidenti.

Sa i perket menyres se plotesimit te fushes "Numri i perdoruesve", ne Aneksin 1, propozojme ne qe vleresimi i numrit total te persoruesve te prekur te behet duke marre parasysh numrin e perdoruesve te cileve nje stacion i sherben ne 24 ore/ si mesatare e nje muaji.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e A dhe se eshte ne gjykimin dhe vleresimin e operatorit qe te jap nje numer te perafert te perdoruesve ne rastet kur nuk eshte e mundur vleresimi i sakte i numrit te pajtimtareve te prekur.

Sipërmarrësi B

Tek pjesa" Fushat e Formularit të raportimit të incidenteve" termi autoritetet rregullatore duket sikur është përdorur gabim në vend të termit "operator"

Qëndrimi i AKEP:
AKEP ben me dije se termi "autoritetet rregullatore" eshte perdorur ne menyre te sakte.

Aneksi 2

Sipërmarrësi A

Ne Aneksin 2 "Tabela per vleresimin e impaktit te incidentit te sigurise", ne seksionin e pare "kohezgjatja e incidentit te sigurise", propozojme qe "vjedhja" te hiqet pasi kohezgjatja e saj nuk mund te matet.
Gjithashtu, ne perputhje mesa kemi komentuar ne piken 10 me siper te komenteve tona, propozojme qe impakti lidhur me numrin e perdoruesve te ndahet ne mesatar dhe te larte si me siper.

Qëndrimi i AKEP:
AKEP merr ne konsiderate propozimin e A duke e hequr termin "vjedhja" nga seksioni i pare ne Aneks 2 dhe duke bere ndryshimet perkatese ne rregullore.

Sipërmarrësi B kerkon qe aneks2 te riformulohet si me poshte:

TABELA PER VLERESIMIN E IMPAKTIT TE INCIDENTIT TE SIGURISE		
Kohezgjatja e incidentit te sigurise(nderprerjes se sherbimit, interceptimit te komunikimeve, softëare te demshem, vjedhja, modifikimi i te dhenave)	Me teper se 1 ore, por me pak se 2 ore	Me teper se 4 ore
Numri i perdoruesve te prekur nga incidenti ose % e tyre ndaj numrit total te perdoruesve te ofruesit		
>1000 ose <5%	I Ulet	Mesatar
Ne rast te nje numri te panjohur te perdoruesve te prekur nga incidenti i sigurise, zona gjeografike e shtrirjes se incidentit te sigurise		
>10 km²	Mesatar	I Larte
Vleresimi Perfundimtar i Impaktit:	Mesatar	I Larte

Qëndrimi i AKEP:
AKEP i qendron percaktimeve dhe parametrave sipas ANEKS 2 "TABELA PER VLERESIMIN E IMPAKTIT TE INCIDENTIT TE SIGURISE"

Aneksi 3

Sipërmarrësi B Albania

Pika SO1- . masat e sigurisë pika 2.e dhe SO 4 – pika 2 D. Rishikimi i politikës së sigurisë pas çdo incidenti nuk mund të jetë mandator dhe shpesh është i panevojshëm. Detyrimi për të riparë politikën apo çdo dokument tjetër pas çdo incidenti, duhet të jetë vetëm nëse investigimi ka nxjerrë si konkluzion nevojën për përditësim.

Qendrimi i AKEP:
AKEP merr ne konsiderate komentin e operatorit B, pika 2 e), SO1 ndryshon dhe behet si me poshte vijon:
"Rishiko politikën e sigurisë pas incidenteve nese konsiderohet e nevojshme."

AKEP merr ne konsiderate komentin e operatorit B, pika 2 d), SO4 ndryshon dhe behet si me poshte vijon:
"Rishiko politikën e sigurisë për palët e treta, pas incidenteve ose ndryshimeve nese konsiderohet e nevojshme"

Sipërmarrësi B kerkon qe aneks 3 te riformulohet si me poshte:

D5: Menaxhimi I Incidenteve
SO 17: Procesi i Zbulimit të Incidenteve

Qendrimi i AKEP :
AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimet perkatese.

D6: Menaxhimi I Vazhdimit të Biznesit

SO 19: Strategjia e Vazhdimit të Shërbimit dhe Disaster Recovery

Qendrimi i AKEP :
AKEP i qendron percaktimit te pikes SO19 ne Aneks 3.

SO 20: Aftësia e Rregullimit të Pasojave

Qendrimi i AKEP :
AKEP i qendron percaktimit te pikes SO20 ne Aneks 3.

SO 21: Planet e Emergjencës

Qendrimi i AKEP :
AKEP i qendron percaktimit te pikes SO21 ne Aneks 3.

SO 22: Qeverisja dhe Menaxhimi i Riskut

Qendrimi i AKEP :
AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimet perkatese.

	standartet e industrisë. d) Siguro që personeli kryesor përdor metodologjinë dhe mjetet e menaxhimit të riskut e) Rishiko vlerësimet e riskut pas ndryshimeve ose incidenteve. f) Siguro që risqet e mbetura pranohen nga menaxhimi.	*• Udhëzimi për personelin në vlerësimin e risqeve. • Listë e risqeve dhe evidencë e rishikimeve/përditësimeve. • Rishiko komentet ose ndryshimet në vlerësimet e risqeve. • Miratimi dhe aprovimi i menaxhimit për risqet e mbetura.*

Qendrimi i AKEP :
AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimet perkatese.

SO 11: Kontrolli i Aksesit në rrjet dhe sistemet e informacionit

	Masat e Sigurisë	*Evidenca*
1	*a) Përdoruesit dhe sistemet kanë identifikim unik dhe autentikohen dhe autorizohen kur aksesojnë shërbimet ose sistemet.* *b) Implemento mekanizmin e duhur të kontrollit logjik për rrjetin dhe sistemet e informacionit për të lejuar*	• *Loget e aksesit tregojnë identifikues unik për përdoruesit dhe sistemet kur lejojnë ose mohojnë aksesin.* • *Përmbledhje e autentikimit dhe metodave të kontrollit të aksesit për sistemet dhe përdoruesit.*

Qendrimi i AKEP :
Komenti i sipercituar eshte i njejte dhe ne perputhje me percaktimin e kesaj pike ne rregullore.

SO 16: Incident Management Procedures

	Masat e Sigurise	Evidencat
3	d)Investigimi i incidenteve kryesore dhe raportimi i tyre final, duke perfshire veprime lehtesuese te ndermarra dhe rekomandime per te zvogeluar incidente te ngjashme e)Vleresimi i politikave te menaxhimit te incidenteve / procedurave bazuar ne incidente te shkuara.	•Raporte individuale i perballimit te shumices se incidenteve Perditesimi i politikave te menaxhimit / procedurave , rishikim komentesh dhe/ ose ndryshim i logs.

Qendrimi i AKEP :
AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimin perkates.

SO 17 : Aftesia e zbulimit te incidenteve

	Masat e Sigurise	Evidenca
2	b) Implementimi ne sisteme konfigurimet standarde të industrisë dhe procedurat për zbulimin e incidentit. c) Implementimi i sistemeve dhe procedurave për regjistrimin dhe përcjellja incidente ne kohë te njerëzit e duhur.	Sistemet dhe procedurat e zbulimit te incidentit, të tilla si incidentet e Sigurise dhe për Menaxhimin e Ngjarjeve (SIEM) mjete, Helpdesk siguri për personelin, raportet dhe advisories nga kompjuteri Ekipet emergjente Përgjigje (certs), mjetet për vend anomali, e të tjera.

Qendrimi i AKEP :

AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimin perkates.

SO:21 Politikat e Logimit dhe Monitorimit

	Masat e Sigurise	Evidenca
1	a)Imlementimin e monitorimit dhe loggin e te dhenave kritike	•Logot dhe raportet e monitorimit të rrjetit kritik dhe të sistemeve te informacionit.
2	b) Implementon politikën e ngjarjeve dhe monitorimin e sistemeve kritike. c) Vendos mjete për monitorimin e sistemeve kritike d) Vendos mjetet për të mbledhur dhe ruajtur shkrimet e te dhenave kritike.	•Politika te dokumentuara për monitorimin dhe ngjarjet, duke përfshirë kerkesat minimale per monitorimin dhe ngjarjet, periudhën e mbajtjes, dhe objektivat e përgjithshme të ruajtjes monitoringdata dhe shkrimet. • Mjetet për sistemet e monitorimit dhe mbledhjen e logeve

Qendrimi i AKEP :
AKEP i qendron percaktimit te pikes SO21 ne Aneks 3.

Sipërmarrësi D

AKEP ne VKD nr. 2592 shprehet se eshte bazuar per nxjerrjen e kesaj rregulloreje ne nenin 122 te Ligjit nr.9918 date 19.05.2008 "Per komunikimet elektronike dhe postare ne Republiken e Shqiperise", i ndryshuar, i cili trajton masat mbrojtese qe duhet te merren nga sipermarresit ne kuader te mbrojtjes se te dhenave dhe te privatesise.
Por, me tej sqaron se kjo rregullore, perafron Nenin 13 s) Kapitulli III s) te Direktives Kuader 2002/21/EC e amenduar i cili trajton sigurine dhe integritetin e rrjeteve dhe sherbimeve me Nenin 4 te Direktives e-Privacy ne te cilin percaktohet detyrimi per sigurine e rrjetit ne kuader te mbrojtjes se te dhenave personale, duke percaktuar ne objektin e rregullores dhe ne nenet e saj njekohesisht detyrime per sipermarresit si per garantimin e funksionalitetit te rrjetit/sherbimeve ashtu edhe per konfidencialitetin e ofrimit te sherbimeve.
D, gjykon qe keto detyrime duhet te percaktohen ne rregullore te veganta duke specifikuar perkatesisht procedurat respektive. Konkretisht, detyrimi per te marre masa per te garantuar sigurine, integritetin dhe mirembajtjen e funksioneve te rrjeteve te komunikimit elektronik eshte parashikuar ne Nenin 7 pika 3 d) te Ligjit nr.9918, piken 9.1 a) te Aneksit C te Rregullores Nr. 24 date 02.02.2012 "Per Autorizimin e Pergjithshem" si dhe Rregullores nr.31, date 26.12.2013 "Per termat e pergjithshme te kontrates se pajtimit per lidhjen dhe aksesin rrjetin publik te komunikimeve elektronike". Megjithate transpozimi i plote i Nenit 13 s) Kapitulli III s) te Direktives Kuader 2002/21/EC e amenduar, ne lidhje me marrjen e masave per integritetin e rrjeteve dhe vazhdueshmerine e ofrimit te sherbimeve ne keto rrjete, mund te kryhet ne nje rregullore te vecante, pra duke e trajtuar ne menyre te pavarur nga mbrojtja e te dhenave dhe e privatesise.
Ne lidhje me detyrimet mbi masat mbrojtese per te realizuar sigurine dhe integritetin e rrjeteve ne kuader te mbrojtjes se te dhenave dhe privatesise te percaktuara ne Nenin 122 te ligjit nr.9918, piken 9.3 te Aneksit C te Rregullores Nr. 24 si dhe ne Termat e Pergjithshme te Pajtimit, D thekson se i ploteson te gjitha keto detyrime dhe se ka derguar dokumentacionin e plote per zbatimin e tyre prane AKEP me shkresen nr. 51 date 26.01.2015.

Per sa i perket marrjes se masave per sigurine dhe integritetin e rrjetit per vazhdueshmerine e ofrimit te sherbimeve per pajtimtarin, D ka qendrimin e tij dhe komentet perkatese, per i kerkon AKEP se pari parashikimin dhe detajimin e tyre ne nje rregullore te vecante.
Sa me lart, D sugjeron organizimin e nje takimi sqarues nga AKEP me palet e interesuara per trajtimin e problematikave te mesiperme, te cilat i shohim se duhen trajtuar ne menyre te vecante nga njera tjetra, perpara dergimit te komenteve perfundimtare nga palet.

Qëndrimi i AKEP:
AKEP vlereson komentet e derguara nga D por gjykon se keto komente nuk kane te bejne me objektin e ketij konsultimi publik.