“Masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike”

ABISSNET sh.a. (Albanian Business Internet Service Solution Network)
Rr. “Ismail Qemali”. Tiranë - Shqipëri. Tel: +355 44 300 123
sales@abissnet.al/www.abissnet.al

1. Politikat e perdorimit te sigurise se informacionit

1.1 Rishikim i pergjithshem

Qellimet e Pergjegjesit te Sigurise se Informacionit nuk kane si qellim imponimin e kufizimeve te cilat jane ne kundershtim me kulturen e besimit dhe integritetit te Abissnet. Pergjegjesi i Sigurise se Informacionit eshte I angazhuar per mbrojtjen e punonjesve apo partnereve te Abissnet nga veprime ilegale apo demtuese nga individe te ndryshem qofshin keto veprime me dashje apo pa dashje. Te gjitha sistemet, duke perfshire paisjet kompjuterike, software, sistemet operative, paisjet e ruajtjes se te dhenave, mail elektronik, navigimin ne internet(WWW) si dhe FTP(Protokolli i Transferimit te Dhenave) jane prone e Abissnet. Keto sisteme jane per tu perdorur per qellime biznesi dhe qe ju sherbejne interesave te kompanise si dhe klienteve tane. Siguria Efektive eshte nje perpjekje ne grup qe perfshin mbeshtetjen e cdo punonjesi te Abissnet dhe bashkon te gjithe personat te cilet meren me sigurine e informacionit apo sistemet te cilat kane lidhje me te. Eshte pergjegjesi e cdo perdoruesi te kompjutervae te dije keto rregulla mbi sigurine dhe aktivitetet e tyre ne rrjetin e jashtem te jene sipas udhezimeve perkatese.

1.2 Qellimi

Qellimi I kesaj politike eshte qe te nxjerre ne pah limitimet e perdorimit te paisjeve kompjuterike ne Abissnet. Keto rregulla jane vendosur qe te mbrojne punonjesit dhe Kompanine Abissnet. Perdorimi i papershtatshem I ketyre pasijeve e ekspozon Abissnet drejt rreziqeve te ndryshme ne rrjetin e jashtem sic jane sulmet e viruseve, kompromentimi i sistemeve te rrjeteve dhe sherbimeve si dhe probleme ligjore.

1.3 Mbulimi

Kjo politike aplikohet tek te gjithe punonjesit e Abissnet, duke perfshire te gjithe stafin qe ka lidhje me keto paisje apo sherbime. Kjo politike aplikohet ne te gjitha paisjet te cilat jane prone e Abissnet.

1.4 Politikat

1.4.1 Perdorimi i pergjithshem dhe Pronesia

Nderkohe qe nje Administrator Rrjeti i Abissnet krijon nje nivel privatesie te arsyeshem, perdoruesit jane ne dijeni se te dhenat qe ato krijojne ne sistem mbeten prone e Abissnet. Per shkak te nevojes per mbrojtjen e rrjetit, pjesa

menaxhuese duhet te garantoje konfidencialitetin e informacionit i cili ruhet ne cdo paisje rrjeti e cila eshte ne pronesi e kompanise Abissnet. Rasti konkret per kete eshte domain I emaileve qe perdor Abissnet Cpanel ku cdo punonjes ka akses vetem te emaili I tij personal me username dhe password te dedikuar.

Punonjesit jane pergjegjes per te patur nje gjykim sa me te mire dhe te arsyeshem mbi limitin e perdorimit personal te paisjeve ne rrjet. Departamentet individuale jane pergjegjes per krijimin e udhezimeve mbi perdorimin personal te sistemeve. Punonjesit kane akses vetem ne sistemet lokale te cilat kane vetem funksione profesionale sic eshte rasti CRM qe perdoret shtimin e klienteve te rinj, heqjen e tyre,hapjen e problematike qe kane klientet. Asnje nga punonjesit nuk ka akses ne www pasi mund te bien pre e sulmeve te ndryshme. Ky limit eshte bere ne routerin kryesor Mikrotik ku marin akses te gjithe punonjesit e kompanise. Jane krijuar Access Lista qe lejojne vetem komunikmin e brendshem te punonjesve dhe ndalojne dalje e tyre ne internet.

Pergjegjesi i Sigurise se Informacionit rekomandon qe cdo informacion qe perdoruesit e konsiderojne sensitive apo te cenueshem duhet te enkriptohet. Duke qene qe informacioni I vetem qe mund te nxjerre jashte zyrave eshte email I punonjesit ato dergohen te enkriptuar. Kjo gje behet e mundur ne Cpanel nga Administratori I Rrjetit duke zgjedhur opsionin encryption per cdo email qe hostohet nga kompania Abissnet.

Per qellime sigurie dhe mirembajtje te rrjetit individe te ndryshem ne Abissnet monitorojne paisjet, sistemet dhe trafikun e rrjetit ne cdo kohe, kjo gje ne Abissnet mbulohet nga Departamenti NOC(Qendra e Operimit te Rrjetit). Sistemet e monitorimit qe perdor departamenti NOC eshte Observium, Solar Winds. The Dude, Zabbix.

Abissnet ka te drejten qe te auditoje rrjetet dhe sistemet ne menyre periodike ne menyre qe te siguroje perputhshmeri te plote me politikat e permendura me lart.

1.4.2 Informacioni i Sigurise dhe i Pronesise

Informacionin i cili mbahet ne sistemet Internet, Intranet apo Extranet duhet te klasifikohet si konfidencial apo jo konfidencial. Punonjesit e kompanise ndermarin hapat e nevojshem ne menyre qe te ndalohet aksesi i pa autorizuar drejt ketyre informacioneve. Te gjithe informacionet jane te ruajtura ne nje FTP Server dhe jane te mbrojtura me password. Punonjesit mund ti lexojne keto te dhena por nuk mund ti editojne pasi kane vetem funksion Read. Departamentet jane te ndara ne VLAN te vecanta dhe secili department ka akses vetem ne filet personale te atij departamenti. P.sh departamenti I AARR mund te editoje vetem filet te cilat ndodhen ne ate VLAN qe eshte ai department dhe per me teper jane te mbrojtura edhe me password.

Password-et mbahen te sigurte dhe nuk ndahen me punonjesit e tjere te kompanise dhe aq me teper me te trete jashte kompanise. Perdoruesit e autorizuar jane totalisht pergjegjes per sigurine e password-eve apo llogarive te

tyre. Cdo kater muaj ndryshohen password-et nga i gjithe staffi i Abissnet ne menyre qe te rritet siguria, gjithashtu cdo tre muaj ndryshohen password-et e paisjeve sistemeve apo paisjeve kryesore ne rrjetin Abissnet.secili punonjes per tu future ne rrjetin e brendshem ne Abissnet duhet te lidhet me VPN me nje username dhe password te caktuar ku nepermjet kesaj VPN ka aksese te percaktuara ne rrjetin e brendshem Abissnet. Ndarja e ketij password eshte rreptesisht e ndaluar.

Te gjithe kompjuterat, laptopet dhe workstations jane te siguruar me password me nje kohe aktivizimi prej 10 minutash nese ne kete paisje nuk po punohet, ose duke bere log-out menjehere nga perdoruesi i cili do te largohet nga vendi i punes. Kjo behet e mundur nga Active Directory.

Per shkak se informacioni qe mbahet ne komjuterat e levizshem eshte shum i cenueshem, kur transferohet informacion tregohet nje kujdes I vecante. Per kete arsye asnje nga punonjesit nuk lejohet qe te logohet ne rrjetin Abissnet me ane te nje AP jashte ambienteve te kompanise.

Nese nje punonjes i Abissnet, perdor email me domain Abissnet.al per postime ne grupe te ndryshme e ka me detyrim te citoje qe ky eshte nje opinion totalisht personal dhe nuk ka lidhje me politikat qe ndjek Abissnet, pervec rasteve kur postimet jane rrjedhoje e mardhenieve biznesi dhe personi ne fjale eshte i autorizuar te flase ne emer te kompanise.

Te gjithe hostet te cilat jane te lidhura ne rrjetin e brendshem te kompanise Abissnet, qofshin keto ne pronesi individuale apo te Abissnet bejne skanime te vazhdueshme per viruse. Per kete perdoren antivirus Kaspersky Rescue Disk Tool, Avast, Windows Defender.

Punonjesit tregojne nje kujdes te vecante kur hapin emaile nga dergues te panjohur, duke u kujdesur te mos hapin te dhenat te cilat I jane bashkangjitur atij email duke qene se mund te jene viruse te ndryshme.

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

2. Politikat e Sigurise se Server-ave

2.1 Qellimi

Qellimi I ketyre politikave eshte vendosja e standarteve per konfigurimet baze te serverave te brendshem te cilet jane ne pronesi te Abissnet. Implementimet sa me efektive te ketyre politikave do te minimizojne aksesin e pa autorizuar ne informacionet dhe teknologjine e cila eshte ne pronesi te Abissnet. Serverat kane siguri aksesi fizik dhe logjik. Ne datacenter ku ndodhen serverat ka akses vetem nje gurp shume I limituar personash dhe hyrja e ketij grupi ne datacenter eshte e monitoruar se nga kamerat ashtu edhe nga loget e hapjes dhe mbylljes se portes kryesore te datacenter. Aksesi logjik eshte I mbrojtur fillimisht me ane te access listave ku vetem klienti specific ose punonjesi I Abissnet neperjmet IP qe ka mund te kene akses ne keto server per me teper qe jane te mbrojtur me username dhe password specific.

2.2 Mbulimi

Keto politika aplikohen ne paisjet te cilat zoterohen nga Abissnet dhe tek serverat te cilet jane te regjistruar ne pronesi te Abissnet. Keto politika jane specifikishte per paisjet te cilat ndodhen ne rrjetin e brendshem te Abissnet.

2.3 Politikat

2.3.1 Pergjegjesite dhe pronesia

Te gjithe serverat e brendshem ne Abissnet jane ne pronesi te nje grupi operacional I cili eshte pergjegjes per administrimin e sistemit. Grupet operacionale monitorojne perputhshmerine e konfigurimeve ne cdo server. Grupi operacional krijon nje guide per ndryshimin e konfigurimeve, gje e cila pefshin rishikimin dhe miratimin nga Pergjegjesi I Sigurise se Informacionit.

- Serverat regjistrohen ne sistemin e menaxhimit te korporates.

Minimalisht kerkohet informacioni I meposhtem ne menyre qe te identifikohet ne menyre te sakte pika e kontaktit.

- Vendodhja dhe nje kontakt I serverit dhe nje kontakt reserve.
- Version I Sistemit te Operimit dhe atij Fizik.
- Funksionet dhe aplikacionet kryesore.
- Informacioni ne sistemin e menaxhimit te korporates mbahet I perditesuar.
- Ndryshimet ne konfigurimin e serverave duhet te ndjekin procedurat perkatese te ndryshimeve perkatese.

2.3.2 Udhezimet per konfigurimet e pergjithshme

- Konfigurimet e sistemeve te operimit duhet te jene ne perputhshmeri me udhezimet e miratuara nga Pergjegjesi I Sigurise se Informacionit.
- Sherbimet dhe aplikacionet qe nuk perdoren caktivizohen.
- Aksesi ne sherbime regjistrohet dhe mbrohet me ane te metodave te kontrollit te aksesit.

- Instalohen patch-et e sigurise me te fundit.
- Serverat jane fizikisht te vendosur ne nje ambient te kontrolluar.
- Serverat nuk duhet te jene te vendosura ne dhoma te vogla, por ne Abissnet jane te vendosur ne dhoma me hapesire te madhe dhe me ajer te kondicionuar dhe me lidhje redundante.

2.3.3 Monitorimi

- Te gjitha eventet qe kane lidhje me sigurine e sistemeve duhet te regjistrohen si me poshte:
  - Te gjitha regjistrimet te cilat kane lidhje me sigurine mbahen online per te pakten nje jave.
  - Backup I konfigurimeve I perditshem duhet ruhet deri te pakten 1 muaj.
  - Nje backup I plote I te gjitha regjistrimeve te sistemeve te nje jave mbahet te pakten per nje muaj.
  - Backup-e te plota te nje muaji ruhen per te pakten 2 vite.

- Eventet qe kane lidhje me sigurine raportohen tek Pergjegjesi I Sigurise se Informacionit, I cili me pas rishikon regjistrimet qe ka sistemi dhe raporton me pas tek menaxheri I IT. Eventet qe kane lidhje me sigurine perfshine:
  - Sulmet nga skanimi I portave
  - Akses I padeshiruar tek llogarite e privilegjuara.
  - Ndodhi jo normale ne lidhje me aplikacionet ne nje host te caktuar.

2.3.4 Zbatimi

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

3. Politikat e Perdorimit te Email-eve

3.1 Qellimi

Me qellim parandalimin e prishjes se imazhit te kompanise Abissnet nga emailed qe dalin nga Abissnet, publiku I gjere tenton ti shikoje keto mesazhe si nje deklarate zyrtare nga ana e Abissnet.

3.2 Mbulimi

Kjo politike merret me perdorimin e duhur te cdo email qe dergohet nga adresat email Abissnet dhe aplikohet mbi te gjithe punonjesit e Abissnet. Cdo punonjes ka ne fund te emailit te konfiguruar signature e tij me emrin e Abissnet dhe poziocionin e punes qe ushtron.

3.3 Politikat

3.3.1 Perdorimi I ndaluar

Sistemi I email-eve ne Abissnet nuk perdoret per krijimin apo shperndarjen e mesazheve me permbajtje ofenduese mbi rracen, gjinine, ngjyren, moshen, orientimet seksuale, pornografi, besimet fetare, besimet politike apo mbi origjinen kombetare. Punonjesit te cilet marin ndonje email I cili ka permbajtje te ngjashme me rastet e permendura me lart raportojne menjehere tek supervizori.

3.3.2 Perdorimi personal

Perdorimi I nje sasie te arsyeshme te burimeve te Abissnet per email-e personale eshte e pranueshme, por keto emaile qe nuk kane lidhje me punen duhet te ruhen ne nje folder te vecante. Ne cdo email te konfiguruar eshte mundesi qe brend folderit Inbox apo Sent te krijohet nje folder I vecante per emailet qe nuk kane qellime funksionale me punen. Dergimi I email-eve jo serioz nga llogaria Abissnet eshte e ndaluar. Sa here qe dergohet nje email I ri, fillimisht duhet te kaloje kontrollin e antivirus-it, me pas eshte I sigurt per tu derguar nga llogaria Abissnet drejte llogarive te tjera. Keto kufizime jane te aplikueshme dhe per email-et te cilat I jane derguar nje punonjesi Abissnet dhe I cili do ta ridergoje kete email ne nje llogari tjeter brenda apo jashte Abissnet.

3.3.3 Monitorimi

Punonjesit e Abissnet nuk presin privatesi ne informacionin qe ato ruajne, dergojne apo marin ne sistemin e email te kompanise. Abissnet monitoron mesazhet pa patur nevoje te njoftoje punonjesit per kete gje. Kjo gje realizohet neperjmet Cpanel. Abissnet nuk eshte I detyruar te monitoroje mesazhet e derguara me email.

3.3.4 Zbatimi

punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

4. Politikat e medias se levizshme

4.1 Rishikim I pergjithshem

Media e levizshme eshte nje burim I njohur I infektimeve me viruse dhe lidhet direkt me humbje te informacionit ne shume organizata.

4.2 Qellimi

Per te minimizuar riskun e humbjeve apo te ekspozimit te informacionit qe mbahet nga Abissnet gjithashtu dhe reduktimi I riskut te marjes se viruseve ne kompjuterat te cilat operojne ne Abissnet.

4.3 Mbulimi

Kjo politike mbulon te gjithe kompjuterat dhe serverat te cilet operojne ne Abissnet.

4.4 Politikat

Stafi I Abissnet mund te perdore median e levizshme vetem ne kompjuterat e tyre te punes. Media e levizshme e Abissnet nuk duhet te lidhet apo te perdoret ne kompjutera te cilet nuk zoterohen nga Abissnet apo pa lejen e Abissnet. Informacioni sensitive duhet te ruhet ne media te levizshme vetem kur eshte I specifikuar ne detyrat e punes, ose ne ato raste kur kerkohet informacion nga organizatat qeverisese. Perjashtime nga keto rregulla behen vetem ne rastet kur behen me kerkese te vecante dhe vetem per ceshtje specifike.

4.5 Zbatimi

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

5. Politikat e password-eve te DB (Data Base)

5.1 Qellimi

Keto politika vendosin kerkesat per ruajtjen dhe marjen e username nga databaza ne menyre te sigurte, keto username do te perdoren per te aksesuar nje nga paisjet te cilat ndodhen ne rrjetin Abissnet. Programet kompjuterike te cilat operojne ne rrjetin Abissnet shpesh qe te operojne ne menyre te plote kane nevoje per nje nga databazat e brendshme te rrjetit Abissnet. Ne menyre qe te aksesoje keto databaza , nje program duhet te autentikohet ne database duke paraqitur kredenciale te vlefshme. Keto kredenciale I jepen punonjesit pasi ka kaluar nje periudhe trajnimi dhe pasi eshte vendosur punesimi I tij.

5.2 Mbulimi

Kjo politike aplikohet tek te gjitha programet te cilat do te aksesojne databazen e perdoruesave.

5.3 Politikat

5.3.1 Te pergjithshme

Me qellim mirembajtjen e sigurise se databazes se brendshme te Abissnet, aksesi I programeve soft do te lejohet vetem pas autentikimit te suksesshem me kredencialet perkatese.Kredencialet te cilat do te perdoren per autentikim ne kete database nuk duhet te jene te ruajtura ne tekst ne kodin e programit por te enkriptuara. Kredencialet e databazes nuk duhet te ruhen ne nje vendodhje e cila eshte e aksesueshme nga web. Konkretisht ne Abissnet secili punonjes mund te aksesoje sisteme e Abissnet vetem me kredencialet e tij.

5.3.2 Kerkesa Specifike

Ruajtja e username dhe password te databases

- Username dhe password te databazes ruhen ne nje dokument te vecante nga pjesa e kodit te ekzekutimit te programit. Ky dokument nuk eshte I lexueshem jasht rrjetit te Abissnet pasi eshte I ruajtur ne nje kompjuter specifik nga nje perdorues qe merret me menaxhimin e serverave.
- Kredencialet e databazes jane te ruajtura ne serverin e databazes.

Marja e username dhe password nga databaza

- Nese username dhe password jane te ruajtura ne nje dokument qe nuk eshte kodi kryesor, atehere keto te dhena lexohen nga nje file tjeter qe eshte I ruajtur ne kete database.
- Hapesira ku do te ruhen keto user dhe password eshte e ndare fizikisht nga pjesa tjeter e programit.

Aksesi ne databazen e username dhe password-eve
- Cdo program apo cdo koleksion programesh ka kredencialet e tij unike ne database. Ndarja e kredencialeve ndermjet programeve te ndryshme nuk lejohet. P.sh program I finances mund te aksesohet nga perdoruesi vetem me username dhe password e tij perkates te cilat vendosen nga menaxheri I departamentit.. Pa keto kredenciale eshte e pamundur qe te aksesohet.
- Password-et e databazes te cilet perdoren nga programet kane nivele te
ndryshme.

5.4 Zbatimi

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

6. Politikat e extranet

6.1 Qellimi

Ky document pershkruan politikat nepermjet te cilave palet te treta lidhen me ane te rrjetit Abissnet me qellim nderlidhjeje ndermjet bizneseve.

6.2 Mbulimi

Ne kete politike perfshihen pale te treta te cilat kerkojne akses ne burimet jo publike te Abissnet pavaresisht menyres se perdorur per te bere lidhjen qofte ajo me VPN apo me qark te thjeshte si psh ISDN apo frame relay. Lidhja me pale te treta sic jane kompanite e ofrimit te sherbimit te internetit te cilat ofrojne akses ne internet per kompanine Abissnet nuk jane pjese e ketyre politikave.

6.3 Politikat

Kerkesat paraprake
- Te gjitha lidhjet e reja extranet kalojne ne nje faze rishikimi ne bashkepunim me departamentin e sigurise se informacionit, ku rishikimet kane te bejne me permbushjen e plote te kerkesave te biznesit per te patur nje siguri sa me te larte.
- Per cdo lidhje te re qe behet firmoset nje marreveshje ndermjet Abissnet dhe paleve te treta te interesuara per te mare sherbime nga Abissnet. Kjo marreveshje firmoset nga zevendes presidenti I kompanise Abissnet dhe nga perfaqesues te paleve te treta.

- Nga kompania Abissnet vendoset nje pike kontakti per palet e treta te cilet kerkojne keto sherbime nga Abissnet dhe te gjitha ceshtjet ne lidhje me kete klient ndiqen nga kontakti I vendosur.

6.4 Zbatimet

Cdo punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes.

7. Rrjetet Virtuale Private (VPN)

7.1 Qellimi

Qellimi I ketyre politikave eshte qe te siguroje udhezime per aksesin remote ose lidhej virtuale private drejt rrjetit Abissnet.

7.2 Mbulimi

Kjo politike zbatohet mbi te gjithe punonjesit e Abissnet duke perfshire dhe personelin qe ka lidhje me pale te treta te cilat perdorin VPN per te aksesuar rrjetin e brendshem te Abissnet.

7.3 Politikat

- Punonjesit e Abissnet mund te perdorin VPN per te punuar nga shtepite e tyre ne raste emergjente, kur duhet te behet nje nderhyrje e shpejte ne rrjet apo kur duhet te modifikohen dokumenta te ndryshem.
- VPN perdoret nga punonjesit Abissnet duke perdorur kredencialet e tyre unike ku perfshihet nje username dhe nje password I forte ne menyre qe te realizojne lidhjen me Abissnet. Kjo mundesohet nga account qe ka secili punonjes brenda rrjetit te zyrave. Nuk duhet ne asnje rrethane keto te dhena te ndahen apo te perdoren nga te tjere pasi te gjitha masat
ndeshkuese do te bien mbi username perkates dhe jo mbi personin I cili
ka shkaktuar demet perkatese nga nje nderhyrje e pa deshiruar.
- Punonjesit te cilet mund te perdorin VPN marin aprovimin me pare nga
pergjegjesi I sigurise se informacionit. Kjo gje kontrollohet pasi mund te caktivizohet servisi I punonjesit ne routerin qendror te zyrave.
- Te gjithe kompjuterat qe perdoren per te bere lidhjen VPN duhet te jene
te update-uar me antiviruset me te fundit.

- Te gjitha te dhenat e VPN dhe gateway konfigurohen ne paisjen baze te rrjetit te zyrave nga administrator I rrjetit.

7.4 Zbatimet

punonjes I cili thyen politikat e permendura me lart do te jete pjese e ndeshkimeve disiplinore duke shkuar deri ne shkeputje te mardhenies se punes

8. Menaxhimi I Riskut.

a) Identifikimi dhe vlerësimi i aseteve kritike të informacionit

1. Risqe per arsye fizike ambjentale

1.1 Demtim HDD

1.2 Demtim i pergjithshem ne Server CPU / Memory – Server offline

1.3 Mungese energjie ne datacenter

1.4 Probleme me bllokun e ushqimit te serverit

1.5 Probleme me furnizimin / linjen e furnizimit me energji te serverit

1.6 Server jo-operacional per shkak te temperatures se larte ne ambjent ose per shkak te demtimit te sistemit te ventilimit/ftohjes ne server.

1.7 Demtim / Vjedhje teresore/pjesore e serverit

1.8 Shkaqe / Fuqi te mbinatyrshme, Zjarri, Permbytja etj ne Datacenter

2. Risqe per shkak te nderhyrjeve (Hacking)

2.1 Sulm DoS (Denial of Service) Trafik i larte

2.2 Sulm DoS ndaj nje sherbimi te caktuar (psh drejt serverit DNS)

2.3 Akses i pautorizuar nga jashte i nje serveri me IP publike (root access)

2.4 Akses i Paautorizuar nga brenda I nje serveri me IP private

2.5 Korruptim, fshirje e te dhenave ne database.

3. Risqe per shkak te gabimeve njerezore.

3.1 Fshirje, modifikim te dhenash per klientin ne menyre te gabuar

3.2 Fshirje teresore/pjesore e te dhenave gjate update-ve apo gabimeve ne kod (programim)

3.3 Publikim I te dhenave per kliente / grup klientesh me dashje nga stafi

3.4 Publikim I te dhenave per kliente / grup klientesh gjate update-ve apo gabimeve ne kod (programim)

b) Vlerësimi i riskut

Probabiliteti	Rrezikshmeria				
	Sh. I ulet	I ulet	I mesem	I larte	Sh. i Larte
Shume i vogel	3.4	3.2	1.6 , 2.5	2.3 , 2.4	1.2, 1.3 ,1.7, 1.8
I vogel		3.3		1.4 , 1.5	
I mesem	3.1	1.1	2.1, 2.2		
I larte					
Shume i larte					

c) Trajtimi i riskut

1.1 Demtim HDD

Cdo server ka sistem raid 10 N+2 pra demtimi i deri 2 HDD nuk nderpret vijimesine e punes.

1.2 Demtim i pergjithshem ne Server CPU / Memory – Server offline

- Serverat jane Industrial Grade me MTBF (Mean Time Between Failure) shume te larte. Serverat zevendesohen periodikisht cdo 5 vjet.

1.3 Mungese energjie ne datacenter

- Sistem UPS me Bateri deri ne 6 ore. Gjenerator automatic me autonomi te karburantit deri ne 48 ore

1.4 Probleme me bllokun e ushqimit te serverit

- Cdo server me 2x Blloqe ushqimi

1.5 Probleme me furnizimin / linjen e furnizimit me energji te serverit

- Cdo bllok ushqimi furnizohet nga nje linje e vecante energjie.

1.6 Server jo-operacional per shkak te temperatures se larte ne ambjent ose per shkak te demtimit te sistemit te ventilimit/ftohjes ne server.

- Temperatura ne datacenter sigurohet nepermjet 2 sistemeve AC te dubluar. Serverat jane Industrial Grade

1.7 Demtim / Vjedhje teresore/pjesore e serverit

- Akses fizik I kontrolluar. Kontroll I jashtem ne recepsion, Hyrje me smart card, dere e blinduar. Survejim me kamera ne ambjentin e jashtem dhe te brendshem.

1.8 Shkaqe / Fuqi te mbinatyrshme, Zjarri, Permbytja etj ne Datacenter

- Datacenter eshte ne kuote mbi 8m nga toka, nuk ka ne afersi tuba te shkarkimit te ujrave. Temperatura dhe prania e tymit detektohet nepermjet sensoreve dhe gjenerohen SMS dhe E-mail. Monitorim 24x7 me kamera nga staf I dedikuar.

2. 2.1 Sulm DoS (Denial of Service) Trafik i larte
   - Monitorim I trafikut me ane te Netflow Analyser. Identifikimi I burimeve te sulmit dhe bllokimi ne piken e hyrjes ne rrjet apo ne provider.

2.2 Sulm DoS ndaj nje sherbimi te caktuar (psh drejt serverit DNS)
   - Monitorim I trafikut me ane te Netflow Analyser. Identifikimi I burimeve te sulmit dhe bllokimi ne piken e hyrjes ne rrjet apo ne provider. Shtimi I makinave te tjera virtuale per te ndare trafikun

2.3 Akses i pautorizuar nga jashte i nje serveri me IP publike (root access)
   - Firewall qendror ne routerin kryesor si dhe firewall i personalizuar ne cdo server qe mundson aksesin vetem nga IP te percaktuara edhe nese njihet password-i.

2.4 Akses i Paautorizuar nga brenda i nje serveri me IP private
   - Firewall qendror ne routerin kryesor si dhe firewall i personalizuar ne cdo server qe mundson aksesin vetem nga IP te percaktuara edhe nese njihet password-i.

2.5 Korruptim, fshirje e te dhenave ne database.
   - Databaza eshte me IP private, potencialisht e pa aksesueshme nga jashte. Firewall I personalizuar.

3. 3.1 Fshirje, modifikim te dhenash per klientin ne menyre te gabuar
   - Akses tek databaza e klienteve kane vetem departamenti i NOC dhe ata mundet vetem te modifikojne te dhenat teknike te logimit dhe te vendndodhjes se klientit. Cdo veprim logohet dhe ruhet ne sistem ne menyre permanente.

3.2 Fshirje teresore/pjesore e te dhenave gjate update-ve apo gabimeve ne kod (programim)
   - Perpara cdo ndryshimi ruhet nje kopje e databazes ne menyre qe ne cdo rast mund te behet revert ne gjendjen e meparshme.

3.3 Publikim I te dhenave per kliente / grup klientesh me dashje nga stafi
   - Vetem nje staf i kufizuar ka akses ne te dhenat e klienteve. Nuk egziston mundesia e gjenerimit te listave apo export te te dhenave. Cdo veprim logohet.

3.4 Publikim I te dhenave per kliente / grup klientesh gjate update-ve apo gabimeve ne kod (programim)
   - Sistemi i te dhenave te klienteve eshte me IP private dhe eshte I aksesueshem vetem nga brenda rrjetit te zyrave.