MOBX TELECOM SHPK

Kompania Mobx Telecom nuk ka filluar akoma sherbimin e telefonise fikse dhe sherbimin internet por ka parashkuar masat e nevojshme per sigurine.

MASAT E PARASHIKUARA PER SIGURINE E SHERBIMEVE

Meqenese kompania jone do te perdore rrjetet/linja me qera te operatoreve te tjere te rrjeteve, qe do te ofroje sherbime internet dhe telefoni fikse, eshte e qarte se shumica e masave te sigurise se rrjetit do te zbatohen nga kompanite ISP qe do tu perdorim rrjetin por ne do tu pershtatemi plotesisht rregullave te tyre te sigurise.

Pjesa tjeter e masave te sigurise qe ka te beje me pajisjet fundore dhe komunikimin dhe vazhdimin e sherbimeve, do te mundesohetnga kompania jone.

Me poshte paraqesim politikat e sigurise se sherbimeve qe do te aplikohen:

Qeverisja dhe Menaxhimi i Riskut

Te gjithe punonjesit e kompanise time jane subjekt i nje kontrolli vjetor per te siguruar zbatimin e rregullave dhe standardeve te sigurise dhe per te pasur nje risk te ulet me qellim menaxhim me te mire te tij. Te gjitha pajisjet dhe rrjeti kontrollohen nga tekniket dhe pergjegjesi i rrjetit per problemet e sigurise.

Keto kontrolle perfshijne ekzaminimin e sistemeve operacionale per t'u siguruar qe kontrollet e sigurise te pajisjeve dhe te programeve jane implementuar me korrektesi.

Punonjesit jane pergjegjes per mbrojtjen dhe trajtimin me kujdes te pasurive te kompanise. Te gjitha llojet e informacioneve mbrohen me sisteme me standart te larta te sigurise si nga prodhuesit edhe nga instalimet tona.

Personi pergjegjes per risqet ka per detyre zbulimin dhe identifikimin e kercenimeve perpara se ato te ndodhin duke bere te mundur planifikimin dhe

veprimtarine parandaluese gjate kohes kur nje proces, aktivitet apo sherbim eshte duke u ekzekutuar.
Personi pergjegjes per risqet zbaton nje procedure standarte per identifikimine e kercenimeve dhe raportimit menjehere te Administratori.

Siguria e Burimeve Njerezore

Pergjegjesi teknik i sigurise:

Detyre e Pergjegjesit teknik te sigurise eshte te krijoje, te implementoje dhe te mirembaje nje programacion sigurie qe te ndihmoje kompanine ne mbrojtjen e informacionit.

Pergjegjesi teknik i sigurise do te jete pergjegjes per:

- krijimin, per te gjithe kompanine, te standardeve dhe te udhezuesve per sigurine e informacionit dhe sigurine fizike;
- permiresimin e vazhdueshem te ketij udhezimeve per stafin;
- imponimin e zbatimit te rregullave per ruajtjen e standardeve te sigurise;
- zhvillimin dhe kryerjen e nje sensibilizimi te vazhdueshme per sigurine per
  ndergjegjesim e punonjesve te kompanise;
- trajnimin e personelit ne lidhje politikat dhe me procedurat e sigurise ne system;
- kryerjen dhe permiresimin e vazhdueshem (te pakten nje here ne vit) te analizes se riskut;
- rishikimin e vazhdueshem (nje here ne muaj) te te drejtave te aksesimit te
  informacioneve;

- rishikimin e vazhdueshem (nje here ne gjashte muaj) te masave te sigurise ndaj ofruesve te sherbimeve te jashtme, veçanerisht personelit qe punon me kontrate ne ambientet e kompanise;
- rishikimin e rregullt (nje here ne muaj) te privilegjeve per aksesimin e sistemeve te kompjuterave;
- kontrollin per heqjen e menjehershme te llogarive te perdoruesve qe japing
  doreheqjen ose largohen nga puna per arsye te tjera;
- drejtimin e kontrolleve te sigurise, perfshi ketu organizimin e rregullt te kontrolleve te jashtme;
- shqyrtimin e thyerjeve te sigurise qe raportohen;
- raportimin rregullisht (te pakten nje here ne muaj) tek Administratori mbi
  gjendjen e sigurise.

Te gjithe punonjesit e kompanise do te instruktohen ne lidhje me menyrat e krijimit dhe administrimit te fjalekalimeve per zgjedhjen e fjalekalimit fillestar, ndryshimin e fjalekalimit dhe keshilla te njohura sigurie per zgjedhjen e tij, mbrojta e fjalekalimit si dhe ndalimi i dhenies se fjalekalimit midis perdoruesve, inicializimi ose mbivendosja e fjalekalimit (ne qofte se nje llogari perdoruesi eshte mbyllur ose ne qofte se perdoruesi ka harruar fjalekalimin).

Mbivendosja e fjalekalimit behet vetem nga personi i autorizuar i teknologjise se informacionit pas nje kerkese me shkrim.

Perdoruesve u kerkohet ne kontrate te pranojne se ata i kane lexuar dhe i kane kuptuar rregullat dhe qe do t'i zbatojne ato.

Kjo proçedure perfshihet ne procedurat e punesimit dhe trajnimit te personelit te kompanise.

I gjithe personeli i kompanise time eshte pergjegjes per respektimin dhe per ruajtjen e nivelit te kerkuar te sigurise gjate kryerjes se detyrave. Ai vepron

vazhdimisht ne perputhje me udhezimin per parimet dhe rregullat e pergjithshme te sigurise se informacionit.

Personat, te cilet nuk jane punonjes te kompanise, nuk lejohen te aksesojne ne asnje moment pajisjet dhe pasurite e kompanise.

Bejne perjashtim vetem persona te autorizuar ne shkrim nga autoritetet e ngarkuara me Ligj dhe ata ne prani te Administratorit.

Administratori eshte personi pergjegjes per mbajtjen e te dhenave ne lidhje me te gjitha aksesimet e autorizuara, ku perfshihen detaje si : emri i punonjesit, vendi i punes, data, ora dhe dita deri kur i lejohet aksesimi.

Do te jete e detyrueshme mbajtja e logeve/regjistrimeve per te gjitha aktivitetet e aksesimit, kur sistemet e aksesimit te ambienteve e lejojne nje gje te tille.

Personat qe kane akses ne sistemin dhe pajisjet e kompanise jane te detyruar te jene te vetedijshem per rregullat dhe standardet e sigurise.

I gjithe personeli do te marre trajnimin e nevojshem per rregullat dhe per procedurat organizative dhe te sigurise. Ky trajnim do kryhet sa me shpejt qe te jete e mundur pas fillimit te punes se punonjesve te rinj.

Siguria e sistemeve dhe pajisjeve:

Te gjitha pajisjet jo asete te kompanise tone do te mbrohen dhe sigurohen nga kompania qe do na jape rrjetin/pajisjet e sa me qera. Pajisjet fundore tonat, do mbrohen fizikisht nga kercenimet e sigurise dhe nga rreziqet e mjedisit, nga ana jone. Ato do te jene te vendosura ne dhome te mbyllur e te sigurte. Dhoma e pajisjeve pajiset me mjete sigurie te larte, celes me alarm, ajer te kondicionuar, me kamera, me UPS dhe me fikese zjarri.

Te gjitha format e komunikimit ne sistem jane te mbrojtura kunder humbjeve, nderhyrjeve dhe korruptimit dhe rrespektojne privatesine e komunikimit. Lejohet vetem pergjimi i ligjshem nese kerkohet nga autoritetet e ngarkuara me ligj.

Te gjitha te dhenat sensitive te sistemit do u behet *backup* (kopje) i rregullt ne perputhje me procedurat teknike.

Kopjet (backup-et) e te dhenave do ruhen ne vende te mbrojtura nga zjarri dhe jashte ambienteve ku mbahen serverat prej te cileve jane marre ato.

Kopjet (backup) e te dhenave do testohen rregullisht per t'u siguruar qe mund te perdoren ne raste te nevojshme.

Procedurat e rikrijimit (restore) te te dhenave do testohen rregullisht per t'u siguruar qe ato jane te efektshme dhe qe ato mund te ekzekutohen brenda kohes se lejuar.

I gjithe personeli i kompanise te cilit do i lejohet akses ne Internet dhe ne sherbim email-i te kompanise por edhe privat me kusht qe te mos marrin viruse duke zbatuar masat e sigurise.

Perdoruesve u jepet akses vetem per logim per te marre sherbimin internet dhe ky akses kontrollohet me rreptesi per te ruajtur integritetin dhe sigurine e sistemit.

Identifikimi i perdoruesit mbulon procedurat per t'u siguruar qe çdo sistem eshte i afte te njohe personat e autorizuar dhe te kryeje veprimet e duhura penguese, ne rastet e perpjekjeve per aksesim te paautorizuar.

Personelit do u ndalohet rreptesisht shperndarja e llogarise personale/klienteve. Thyerja e ketij rregulli do te trajtohet si nje shkelje e rende.

Çdo perdorues do identifikohet ne menyre individuale nepermjet nje llogarie unike perdoruesi, pra nje username dhe password.

Nje llogari unike perdoruesi siguron vetem menyren e autentifikimit per perdoruesit/klientit. Ndalohet rreptesisht dy ose me shume aksesime te njekohshme
me te njejten llogari perdoruesi.

Menaxhimi i Operacioneve

Operacionet jane dy llojesh, operacione pjese e nje sistemi apo sherbimi te ri te planifikuar per implementim dhe operacione te cilat kane funksion mirembajtes, update-ues apo ndryshues ne sistemet ose sherbimet ekzistuese te infrastruktures se rrjetit.

Sherbimet e mirembajtjes se sistemit do jene 100 % efektive ne cdo dite perfshire backup, rikthime backup, etj.
Te gjitha procedurat qe lidhen me teknologjine e informacionit do dokumentohen. Keto do perfshijne, ne menyre te veçante, procedurat e hapjes dhe te mbylljes, *backup*-et dhe mirembajtjen rutine per te gjitha elementet e mjedisit te sistemit dhe rrjetit te kompanise.

Procedurat e operimit do mbulojne si operacionet normale ashtu edhe administrimin e incidenteve te parashikueshme, duke perfshire keqfunksionimin e pajisjeve ose te programeve, te dhenat jo te sakta ose te demtuara, defektet ne pjeset qe i perkasin providerit te internetit, sulmet keqdashese dhe thyerjet e konfidencialitetit.

Menaxhimi i Incidenteve

Incidentet qe do ndikojne mbi sigurine vleresohen me seriozitet dhe raportohen menjehere tek Administratori.

Nje incident sigurie eshte ngjarja e cila mund te ndikoje ne integritetin, disponueshmerine dhe ne konfidencialitetin e informacionit.

Demtimet si pasoje e incidenteve te sigurise dhe te keqfunksionimeve do minimizohen ne maksimum dhe, sa here qe eshte e mundur do parandalohen.

Per te gjitha rastet e ngjarjeve qe lidhen me sigurine do ndiqet nje procedure per raportimin e incidenteve sipas raportimit te percaktuar nga AKEP ne rregulloren e tij.

I gjithe personeli eshte i detyruar per te raportuar çdo dobesi te sigurise ose çdo kercenim te vene re ne procedura, ne sisteme dhe ne sherbime.

Per te minimizuar çdo nderprerje te sherbimit internet apo çdo demtim te te dhenave, do i jepet prioritet si pune qe keqfunksionimi i programeve te korrektohet sa me shpejt qe te jete e mundur.

Keqfunksionimet e dukshme te programeve do i raportohen pergjegjesit, i cili do pergjigjet menjehere dhe udhezon ose nderhyn vete ne raste te tilla.

Kur pergjegjesi apo administratori veren se veprimtaria e nje punonjesi nuk eshte ne perputhje me rregullat dhe procedurat e sigurise, per çfaredolloj arsyeje, ai organizon nje takim me punonjesin per te diskutuar çeshtjen dhe per te planifikuar veprimet korrigjuese te tij ne nje kohe sa me te shkurter.

Menaxhimi i vazhdimit te biznesit

Ne biznesin qe do bejme, varemi si nga ligjet e fushes qe minotorohen nga AKEP, por edhe nga gjendja e tregut te internetit dhe konkurenca ne terren me operatore te tjere.

Themeluesit e kompanise do jene ne konsultime te vazhdueshme me kompanine provider te rrjetit/internetit dhe kompani te tjera ne treg per te pare te gjitha mundesite qe ky lloj biznesi te mos me arrije ne pike kritike dhe pike nderprerje.

Planet tona jane jo vetem per menaxhim te vazhdueshme te biznesit por edhe per ta zgjeruar me tej si sherbim, jo vetem ne ato zona ku jam present por edhe ne zona te reja me rrjet te ri dhe siguri te larte te rrjetit dhe informacionit.

Nderprerje jashte kontrollit tone mund te shkaktohen nga shkaqe natyrore, nga aksidente, nga defekte te pajisjeve, nga veprime te qellimshme ose nga difekte te sherbimeve, por qe masat jane marre me pajisje reserve, me kabllo e fibra reserve, me bateri reserve dhe programe reserve qe nderprerja te jete sa me e shkurter dhe pajisjet apo pjeset e demtuara te rrjetit te zevendesohen ne pak minuta ose 1 ore maksimumi.

Monitorimi, Auditimi dhe Testimi

Pajisjet e rrjetit duke perfshire routerin, switchet dhe modemet kabllore, do gjenerojne informacione prej logeve pra informojne administratorin e rrjetit mbi aktivitetet e kryera ne keto pajisje.

Aplikacionet do identifikojne veprimet e kryera ne to, kohen e kryerjes dhe qellimin prej logeve te regjistruara. Sistemet apo sherbimet do jene te kategorizuar ne elemente te infrastruktures se rrjetit ne te cilat implementohet sistemi i regjistrimit te logeve per aktivitet qe kryhen ne to.

Informacionet qe do gjenerohen nga keto sisteme logesh do jene te ndryshme dhe ja disa prej tyre:

1. IP Addressa e pikave fundore te rrjetit
2. Parametrat teknike te rrjetit per aktivitetin e nje pajisje apo klienti
3. Sherbimi i kryer
4. Ora dhe Data e aktiviteteve
5. Vlerat e trafikut te gjeneruar
6. Veprimtaria e marre nga pajisja per kerkesat e mesiperme

Keto informacione do perdoren ne menyre te vazhduar nga pergjegjesi i sigurise vetem per detyrat e caktuara dhe per te analizuar veprimtarite e meparshme nga sistemet, pajisjet apo sherbimet per vlerat e trafikut te gjeneruar.

Loget e aplikacioneve do ofrojne nje sherbim te rendesishem ne infrastrukturen e kompanise dhe ketu perfshijme loget nga programi i menaxhimit te klienteve Radius Server dhe aplikacionin e tij te faturimit.

Keto informacione do perdoren per te identifikuar anomali, sulme apo sjellje jo brenda standartit te lejuar te pajisjeve, sistemeve apo personave fizike punonjes ose kliente te kompanise.

Sistemet e Logeve do ruajne te dhena deri ne 2 vjet nga momenti i regjistrimit te logeve ne sistem.

Testimet: Ne fazen e kryerjes se testit, regjistrohet me menyrat e percaktuara ne planifikim cdo rekord i kerkuar ne dokumentacionin e testit.

Ne raportin e testit pershkruhen te gjithe procedurat e ndjekura dhe perkrah tyre vlerat e nxjerra nga keto procedura. Gjithashtu pershkruhen konfigurimet e ndryshuara ne sisteme apo sherbime per realizimin e testit si dhe procedurat e kthimit te konfigurimeve ne gjendjen e meparshme.

Faza e fundit e sistemit te testimit eshte kryerja e analizes se vlerave te gjeneruara nga procesi i testimit nga ana e pergjegjesit te sistemit apo sherbimit dhe personit pergjegjes per kryerjen e testimit.

Auditimi: Personi pergjegjes per kryerjen e auditimit e realizon kete proces me kerkese te Administratorit te Kompanise dhe autorizimit me shkrim te tij. Ne rastin kur nje punonjes i kompanise dyshon ne keqfunksionim te nje elementi

te infrastruktures se rrjetit ai i drejtohet personit pergjegjes per kryrjen e auditimit

Personi pergjegjes qe do kryeje auditimin e problemit, perpilon nje dokumentacion mbi raportimin e situatave te zbuluara te cenuesshmerise dhe ia dergon ate Administratorit per te ndermarre veprimet e duhura teknike per te parandaluar riskun e mundshem.

Raport me i gjere masash do te jepet pas fillimit te ofrimit te sherbimeve nga kompani jone.