R&T sh.p.k.
Rr. Luigj Gurakuqi
P. 89, Shk. A
Tel / Fax: +355 4 2274 778
E-mail: info@rt-grp.com
Http://www.rt-grp.com

Drejtuar: **AKEP**

Subjekti: **Siguria ne rrjet dhe masat mbrojtese**

❖ TELEFONIA, INTERNETI DHE SIGURIA

Kompania R&T sh.p.k. ofron sherbimin telefonik dhe shperndarje internet ADSL.
Rrjeti yne eshte reduktuar per shkak edhe te amortizimit te kabllove te bakrit te shtruara para shume vitesh dhe numri i abonenteve eshte ne renie.
Per telefonine ne perdorim nje central Iskra me kapacitet deri 500 pajtimtare por qe aktualisht vetem nje karte 100-she eshte ne pune dhe ka pak abonente telefonie.
Centrali Iskra ka elemente sigurie te vetat dhe eshte i paarritshem nga internet pasi nuk lidhet me internet, por me E1 direkt me Albtelecom ne porten e E1 te centralit. Pra komunikimi i centralit tone eshte i mbyllur vetem me Albtelcom.
Deri sot nuk kemi pasur asnje problem me sigurine e telefonise.

Per internetin perdorim nje ruter Mikrotik edhe ky i lidhur me Albtelecom nga marrim internetin. Ky mikrotik ka firewall te tijin, qe ja kemi bere aktiv dhe kemi bere konfigurimet e nevojshme qe te pengohet cdo sulm drejt rrjetit tone.
Deri sot nuk kemi pasur asnje problem. Kompania Albtelecom ka qene e gatshme te beje konfigurimet ne Mikrotik qe te perputhet me mbrojtjen e sistemit te tyre.

Disa nga funksionet e tij jane:

1. Caktim username dhe password per autentifikim.
2. Implementim firewall per sigurine e të dhënave ne rrjet.
3. Ndarje e rrjetit nga Albtelecom.

Protokollet e punes dhe komunikimit te Mikrotikut:

1. Authentifikimi
2. Fshehtesia
3. Menaxhimi i celesave

Authentifikimi-logimi i cdo user kryhet permes kodit HMAC (Hash based Message Authentication Code) me username dhe password personal. Siguria e ketij kodi varet drejteperdrejt nga siguria e hash funksionit me te cilin eshte llogaritur. Fshehtesia e komunikimit per cdo bit apo ne grupe bitesh, arrihet permes enkriptimit.

Tipari kryesor i tij eshte mundesia e authentifikimit dhe kriptimit te te gjithe trafikut.

Pas pajisjes Miktorik eshte pajisja DSLAM ZTE e cila pershtat sinjalin internet ne linjat dyfillore.
Edhe DSLAM ka mbrojtjen e saj pasi eshte e sinkronizuar ne username dhe password me Mikrotikun dhe i ka te njejta me te.
Sherbimi i internet ofrohet me linjat tona te bakrit. Teknologjia ADSL eshte nje nga menyrat e furnizimit me sherbim Interneti per abonentet kryesisht familjare dhe biznese te vogla. Pavaresisht teknologjise se perdorur per ofrimin e sherbimit, standartet e komunikimit duhet ti nenshrohen modelit ISO/OSI, qe permbledh te gjitha standartet dhe rregullat qe duhet te gezoje nje sistem komunikimi. Nje nga standartet e komunikimit te modelit ISO/OSI eshte i ashtuquajturi niveli i rrjetit qe permban specifikat e struktrurimit dhe menaxhimit te nje rrjeti me shume nyje:

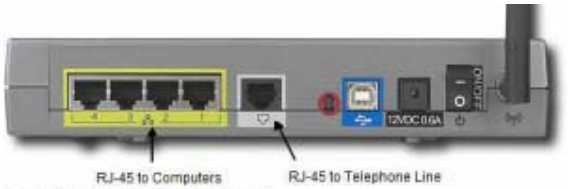
- Modeli i lidhjes. Lidhjet midis nyjeve te rrjetit behen me te ahtuquajturen lidhje te pasigurt. Per shembull protokolli IP eshte standarti me i perdorur per trasmetimin e te dhenave midis nyjeve. Informacioni copezohet ne pjese te quajtura datagrame dhe qe udhetojne nga derguesi drejt marresit nepermjet nyjeve te ndermjetme. Ky protokoll nuk ofron asnje garanci per dorezimin e sigurt te datagrameve, keshtu qe nese nje datagram humbet gjate udhetimit, nuk ekziston asnje mundesi per ta rekuperuar ate.
- Adresimi i hosteve. Me termin host nenkuptojme nje nyje te rrjetit e cila ka aftesine te marre ose dergoje informacion duke per dorur specifikat e nivelit te rrjetit. Per shembull nje host mund te prese ose te dergoje datagrame IP. C'do host ka nje identifikues unik brenda rrjetit ku ben pjese dhe ky identifikues quhet adrese IP dhe perbehet nga nje katershe numrash **a.b.c.d** qe marrin vlera ne intervalin 0-255. Per shembull adresa **192.168.1.1** eshte nje adrese e rregullt IP, nderkohe qe adresa **192.168.1.256** nuk eshte.

- Percjellja e mesazheve. Ne akitekturen bashkekohore te rrjeteve kompjuterike, ku ne krye qendron Interneti (rrjeti i te gjitah rrjeteve), nyjet organizohen ne nenrrjete te lidhura ne rrjete me te medha dhe keto rrjete me te medha mund te nderlidhen me pjesen tjeter te Botes me ane te infrastuktures se Internetit. Per te patur nje prcjellje korrekte te informacionit midis hosteve, nevojiten nyje te posaçme te njohur si router e gateway. Per tu vene ne dukje eshte fakti se edhe keto pajisje te veçanta kane nje identifikues IP brenda rrjetit dhe si te tilla mund te shihen si hoste, ndonese me cilesi te veçanta.

Nyjet

Komunikimi midis hosteve kalon nepermjet disa nyjeve te veçanta ne zoterim te Mikrotik ku klienti ka bere autentikimin dhe pastaj nepermjet nyjeve te veçanta publike qe perbejne infrastukturen e Internetit. Cdo nyje ka nje adrese IP qe e indetifikon ne menyre unike. Per te ndjekur rrugetimin e paketave mund te perdorim aplikacione te ndryshme qe njihen me emertimin traceroute. Ne sistemin operativ Windows, nen promtin e komandave CMD, kemi ne dispozicion komanden tracert. Per shembull nese duam te inspektojme nyjet neper te cilat kalojne paketat nga kompjuteri nga po shkruhet kjo faqe drejt serverit DNS to Google me sdrese IP 8.8.8.8, perdorim komanden tracert 8.8.8.8.

❖ SIGURIA NE RRJETIN TONE ADSL



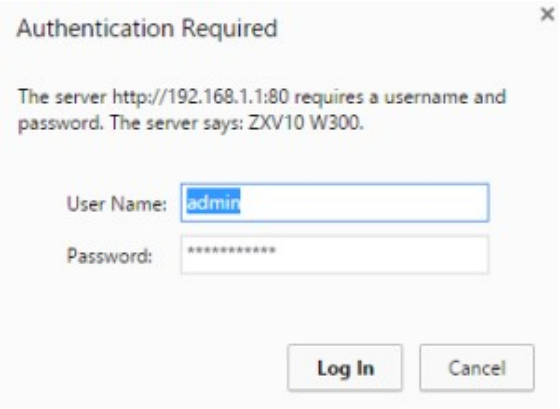
DSL Modem/Router (US)

Lidhja ne rrjet e abonenteve familjare dhe bizneseve te vogla behet me ane te infrastuktures ADSL. Cdo abonent pajiset me nje pajisje modem/ruter ADSL e cila eshte ose TP Link ose ZTE. Ne fakt kjo pajisje nuk eshte thjesht nje modem/ruter por kryen disa funksione:

- Modem: konverton sinjalin analog (qe udheton ne linjen telefonike) ne sinjal dixhital te perdorshem nga nje rrjetkompjuterik.

- Switch: menaxhonpajisjet brenda rrjetit kompjuterik shtepiak te lidhura me kabell apo me vale elektromagnetike (Wireless).
- Gateway: porta e ndermjetme midis rrejtit shptepiak dhe rrjetit te jashtem qe i perket kompanise tone.

Per te konfiguruar parametrat e modemit ose per te diagnostikuar ate na vjen ne ndihme faqja web e administrimit e cila tashme eshte pjese integrale e modemeve bashkekohore. Per te aksesuar faqen web te administratorit, nga browseri i Internetit (Internet Explorer, Google Chrome, Mozilla Firefox etj) hapim adresen lokale te modemit. Per te njohur kete adrese ne Windows, nga CMD perdorim komanden ipcofing e cila na shfaq te gjitha detajet e rrjetit ku nder te tjera do te gjejme edhe nje adrese IP me emertimin Default Gateway. Pikerisht kjo eshte adresa IP e modemit ne rrjetin lokal. Zakonisht kjo adrese eshte 192.168.1.1.



Te njejten gje e bejme edhe duke vendosur adresen IP me te cilen gateway-i shtepiak paraqitet ne rrjetin WAN. Pra nese njohim kete adrese mund te hapim paneli e admistrimit te modemit nga nje cfaredo nyje rrjeti e lidhur ne te njejtin rrjet WAN. Gjitashtu, nga rrejti yne lokal mund te aksesojme panelin e adminstrimit te modemeve te abonenteve te tjere, adresat IP te te cileve mund ti zbulojme ne ç'do moment si u shpjegua edhe me siper.

Per te evituar nderhyrjet nga individe te pautorizuar, modemi kerkon autentikimin me nje emer perdoruesi dhe me nje fjalekalim.

Nje keqberes qe do te kishte akses ne modemin e klientit do te mundohej te nderhynte tek sistemi yne por bllokohet nga Mikrotiku.

Nje nga format qe provojne hackerat eshte qe perpiqen te nderrojne serveri DNS i modemit, duke patur keshtu mundesine e moinorimit te faqeve qe vizitojne abonentet, ose duke i servirur perdoruesve faqe te rreme te cilat mund te permbajne programe malinje qe mund te instalohen brenda kompjutereve ne rrjet. Ne kete skenar, jo vetem qe eshte kompremente uar modemi ADSL, por tashme edhe pajisjet e rrjetit te brendshem quhen pjese e sulmit. Ne kete pike, roli I Mikrotikut eshte mese i mjaftueshem sepse i bllokon shkuarjen me tej ne rrjet.

Ne i kemi instruktuar dhe trajnuar tekniket per tu paraprire ketyre skenareve dhe te informojne klientet per rreziqet qe mund te hasin dhe si mund ti anashkalojne ato.

Ne kemi pergatitur edhe nje document per perdoruesin qe te mos ju nderhyhet ne kompjuterin dhe modemin/ruterin e tyre.

Ne dokument jane edhe disa nga keshillat qe I rendisim:

- Fjalekalimet duhen ndryshuar dhe abonentet duhen instruktuar per te bere vete ndryshimin periodik te fjalekalimeve
- Duhet te mbyllen portat ne anen WAN (si pshm FTP, Telnet, HTTP, SSH, CWMP, SNMP, UPnP etc) per te evituar nderhyrje nga rrjeti i jashtem si ndryshimi i DNS- ve, injektimi i programeve malinje, etj.
- Duhet te shihet mundesia qe ne nje te ardhme personeli teknik i ISP-ve te mund te kete akses te veçante ne modemet e abonenteve me kredenciale te ndryshme nga ato te abonentit, gje qe eshte e pamundur ne modemet ADSL aktual.
- Keshillohen abonentet qe te fikin modemin kur nuk perdorin lidhjen e Internetit.
- Keshillohen abonentet qe te monitorojne trafikun e tyre ditor dhe ne rast se konstatojne trafik jo te zakonshem duhet t enjoftojne personelin teknik te ISP-se.

Nje pjese e ketyre i mundesohen klientit me pajisjen ruter dhe i njoftohen klientit paraprakisht.

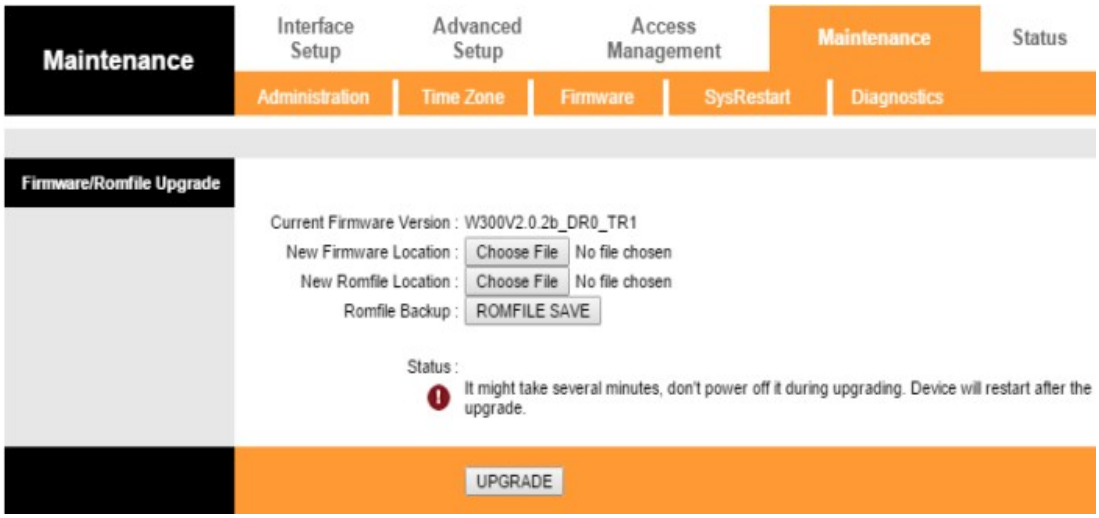
❖ SIGURIA NE PORTAT E PAJISJEVE:

Sic e dime, nje backdoor (porte e pasme) eshte e ngjashme me nje porte sherbimi qe te lejon

tejkalimin e pjesshem ose total te masave te sigurise se nje sistemi kompjuterik. Duke qendruar ne teme, ISP-ja jone qe ofron sherbimin e Internetit per kompjuterin, ka pajisur nje pjese te madhe te klienteve te saj me modem ADSL te markes ZTE.

Per te mos pasur nje backdoor, ne e bllokojme ate ne momentin e konfigurimit dhe modemi ADSL permban një sistem operativ, si dhe një konfigurim (rom) që përmban parametrat më të cilat modemi operon. Sa herë që bëjme risetimin e modemit memoria rom e tij kthehet në gjendjen fillestare të fabrikës. Ndryshimi i parametrave të konfigurimit memorizohet tek rom-i i modemit, i cili mund të shkarkohet në kompjuter ose zëvendësohet nga me një tjetër rom nga kompjuteri. Për të shkarkuar ose zëvendësuar rom-in ose firmware-in e modemit, shkojmë tek webserveri (192.168.1.1:8081) me anë të broëserit dhe mbasi të kemi futur kredencialet, klikojmë Maintainance dhe mandej Firmware.

Na shfaqet:



Në faqe na paraqiteten disa opsione:

- New Firmware: për të karikuar një firmware të ri për ta instaluar
- New Romfile: për të karikuar një rom të ri, pra për të ndryshuar mënyrën e operimit të modemit
- Romfile Backup: për të ruajtur rom-in ekzistues, pra për të ruajtur konfigurimet aktuale

Të gjitha veprimet e mësipërme mundësohen vetëm nëse disponojmë kredencialet e duhura të administratorit. Atëherë ku qëndron problemi?
Modeli ne shqyrtim ofron edhe një mënyrë tjetër për të shkarkuar rom-in ekzistues pa qenë nevoja që të nohim kredencialet e administratorit. Mjafton që në browser të shkruaj adresën http://192.168.1.1:80/rom-0 dhe automatikisht bëhet shkarkimi i romit të modemit në

diskun e ngurtë të kompjuterit, e gjithë kjo pa patur nevojën e autentikimit të administratorit.

Por adresa 192.168.1.1 i përket modemit tim te parë nga rrjeti e LAN tone. Nëse provoj të njëjtën gjë në adresën http://10.22.231.79:80/rom-0 ku 10.22.231.79 është adresa IP që modemi im ka në rrejtin tim WAN, ndodh e njëjta gjë; rom-i i modemit shkarkohet pa problem edhe kur e kërkoj këtë gjë nga ana WAN.
Në këto kushte, sjakrojme rom-et e të gjithë klientëve me përpara se ti dergojme te klienti dhe nuk ka mundesi qe ti behen konfigurime te tjera nga nje hacker dhe as qe te shikohet drejt rrjetit tone nga nje hacker.

Ne jua keshillojme klienteve perdorimin e firewallit dhe antiviruseve edhe per te mundesuar:

1. Monitorimin e faqeve të Internetit dhe listës se tyre, të hapura në mënyrë kronologjike nga punonjësi;
2. Shkarkimin e softeve nga Interneti;

Te gjitha pajisjet jane Mikrotik edhe tek klienti dhe kjo ben qe siguria ne komunikim te jete shume e larte dhe me protokolle te sigurta.

Të gjitha antenat e klienteve kanë password të ndryshëm nga çdo pajisje tjetër në rrjet.

Kur pergjegjesi i sigurise se rrjetit duhet të futet për të kontrolluar sigurine ne komunikim apo per te konfiguruar pajisjen, duhet të dijë "username" dhe "passwordin" e çdo antene, si në LAN ashtu dhe në distance, ku të dy këto passwordet janë të ndryshme.

Gjithashtu konfigurimi i antenave transmetuese është konfigurim ne modem kabllor me protokollin "PPPoe" i instaluar në një PC me system Mikrotik në të cilin janë të ruajtur Userat dhe "username" dhe "password" të ndryshëm për çdo klient.

Këto masa të marra për sigurinë bëjnë që siguria në rrjet të jetë në nivele të larta dhe pritshmëria për thyerje të kodeve është e vogël.

❖ MASA SIGURIE SHTESE PER KLIENTET BIZNES:

Ne u komunikojme klienteve biznes masat per sigurine tone te rrjetit por edhe u mesojme si te ruhen sa me mire ne kompjuterat e tyre, si per shembull:

1. Duhet te aplikojne pajisje me siguri te larte sic jane ruterat Cisco, Mikrotik, etj qe rrjeti i tyre te ruhet sa me mire nga sulmet.
2. Antiviruset ndihmojne sistemin tone por edhe pajisjet e perdoruesit per te rritur dhe maksimizuar sigurine e perdoruesit.
3. Firewallet vendosin mure mbrojtes ndaj sulmeve kibernetike por mbrojtja ne grup me disa menyra mbrojtje eshte menyra me e mire dhe qe do tu rekomandohet klienteve tane.

4. Antiphishing eshte nje menyre per te parandaluar “gjuajtjen” nga servera ose makina robot te cilat duan te hyjne dhe te kapin te dhena ne pajisjet e perdoruesit me qellim futjen e aplikacioneve per te vjedhur te dhenat e tyre si psh te dhena personale, te dhena bankare, etj.
5. Antispyware eshte nje aplikacion qe mbron pajisjen e persoruesit te mos marre programe spiune (spy). Keto programe vjedhin te dhena tek perdoruesi dhe i raportojne ne programet baze te tyre ne distance me anen e internetit. Mbrojtja ndaj spywareve eshte e domosdoshme ne ditet e sotme.

❖ SIGURIA FIZIKE E SISTEMIT

Per te mundesuar Sigurine Fizike kemi marre disa masa:

1. Vendosje e pajisjeve ne ambjente te pershtatshme ne lartesi te konsiderueshme nga toka dhe te paarritshem nga uji.
2. Ruajtje e ambjenteve dhe rrjetit, me punonjes dhe roje 24 ore.
3. Ruajtje e ambjenteve me kamera te cilat i aksesoj dhe shikoj online ne cdo moment nga shtepia dhe celulari.
4. Ruajtja e ambjenteve me sistem alarmi me nje kompani private.
5. Ruajtje e rrjetit nentokesor dhe ajror te fibrave optike apo pjeseve te rrjetit Ethernet, me punonjes gjate orarit te punes.
6. Pajisja me fikese zjarri, e nderrueshme cdo vit.
7. Kondicionim i vazhdueshem 24 ore, per te ruajtur jetegjatesine dhe performance ne punen e pajisjeve.
8. Pajisjet ne tek klienti vendosen ne ambjentet private te tyre dhe ruhen nga klienti 24 ore.

❖ RISKU DHE MENAXHIMI I TIJ

Risqet e jashtme per kete lloj rrjeti qe kemi jane disa:

1. Problemet me energjine elektrike qe ndodh ne disa raste
2. Problemet apo defektet qe mund te japin pajisjet. Ketu fusim dhe dobesite nga ana e sigurise se vete pajisjeve.
3. Mundesia e vjedhjes ose demtimit me dashje,

4. Demtimet nga kushtet atmosferike,
5. Veteamortizimi fizik i pajisjeve, etj,

per te cilat kemi marre masat qe te mos e prekin sistemin tone:

1. Per problemet me energjine elektrike kemi instaluar inverter ne piken e centralit dhe pajisjeve te tjera dhe sistem baterish duke garantuar energji te vazhduar per 8 ore deri ne ardhjen e energjise elektrike. Gjithashtu nje gjerator elektrik me nafte, eshte i gatshem ne cdo moment.
2. Per problemet qe mund te shfaqin pajisjet kam marre keto masa:

a. Nje Mikrotik rezerve me konfigurime te gatshme te njejta me ate ne pune.
b. Konfigurime te gatshme firewall te Mikrotikut per shkurtim kohe ne rast te vendosjes se pajisjes se re.

3. Per te eleminuar vjedhjen dhe demtimin nga keqberes kam marre mas ate ruhen 24 ore pajisjet.
4. Per demtimet nga kushtet atmosferike kam marre masa per tokezimin dhe mbrojtjen nga rrufete me rrufeprites si dhe pajisjet e sistemit jane ne vend te paarritshem nga uji.
5. Per vete amortizimine pajisjeve kam marre masati kem reserve disa nga pajisjet kryesore dhe kam nje find reserve per te blere pajisje te tjera ne rast se prishet ndonjera qe kam ne pune.

Rreziqet e brendeshme jane mos konfigurimi i rregullt i pajisjeve, ose çkonfigurime te pajisjeve qe mund te vijne nga rreziqet e jashtme ose nga pakujdesia ne konfigurime.

Te gjithe keto rreziqe monitorohen vazhdimisht dhe ne cdo moment merren masat e duhura per uljen e nivelit te ketyre rreziqeve.

❖ TRAJNIMET DHE PERSONI PERGJEGJES:

Personi pergjegjes per rrjetin kemi nje person me eksprience shumevjecare ne Albtelecom i larguar nga ajo kompani dhe qe punon per ne. Trajnimet e tij ne Albtelcom I kane sherbyer atij edhe ne punen tone si dhe ka trajnuar stafin per njohurite e nevojshme.

Kemi dhe nje punonjes ndihmes i cili shkon tek klientet ADSL dhe instalon pajisjen atje si dhe kryen konfigurimet per te cilat e kam trajnuar vete.

Duke qene se teknologjia ADSL nuk ka njohur avancime, punonjesit vetetrajnohen ne internet si per konfigurimet e sigurise edhe per modele te reja teknologjish dhe sigurite e tyre.

Edhe kompania Mikrotik jep Help shume te mire dhe te trajnon online per kohen e garancise.

❖ SIGURIA E BURIMEVE NJEREZORE VAZHDIMI I BIZNESIT

Si staf ne jemi dy persona duke qene se klientet jane te paket, njeri pergjegjes dhe tjetri ndihmes, por qe ata jkane e nevojshme per ta mbajtur dhe vazhduar si biznes telefonie dhe interneti. Pavaresisht deshires tone klientet e lene telefonine fikse dhe merren me internetin dhe kjona ka detyruar te konsultohemi shume shpesh me Albtelecom per sherbimin internet dhe te marrim trajnime nga specialistet e Albtelecom, jo ne forme certifikimi por ne forme experience.

Me perpara punonjesi kryesor ka pasur eksperience pune te tille ne kompanine Albtelecom si me telefonine edhe me internetin dhe ai duke pasur eksperiencen e duhur, i ka sherbyer shume kompanise tone dhe na garanton vazhdimin e biznesit pasi i ka mesuar cdo gje edhe ndihmesit dhe ne rast largimi te njerit me leje ose pushime, kemi personin tjeter.

Ndryshimet ne staf nuk kemi pasur keto vitet e fundit por edhe nuk jemi zgjeruar me staf pasi nuk kemi pasur rritje klientesh qe te rrisnim numrin e punonjesve.

Shkeljet ne sigurine e rrjetit nuk tolerohen por arshivohen dhe menjehere i njoftohen administratorit, i cili sjell persona te specializuar te punesuar part-time ose eksperte te Albtelecom-it per te rregulluar problemin, si dhe merren masa qe te mos perseritet si shkelje.

❖ INCIDENTET E SIGURISE

Incidentet sigurie nuk kemi pasur por do incident do te regjistrohet, dokumentohet dhe shqyrtohet ne kohen me te shkurter nga momenti i ndodhjes. Mbahet dhe tabela e incidenteve dhe arshivohet. Tabela e incidenteve ka informacione si:

1. Pershkrimi i incidentit,
2. koha e ndodhjes,
3. koha e verifikimit,
4. permbajtja e incidentit ne detaje,
5. gjurmet ne sistem te tij,
6. path-in,
7. masat per eleminimin e tij
8. mbikqyrje nese perseritet
9. arshivim

❖ MASAT PER ELEMINIMIN E INCIDENTEVE:

1.	Cdo incident vlersohet ne baze te logeve te ruajtura.
2.	Administrohet duke u verifikuar se kush ishte shkaku i incidentit.
3.	Me pas behet analizimi i rrugeve te hyrjes dhe portave te sistemit ne baze te logeve.
4.	Me pas behet mbyllja e ketyre portave.
5.	Rikthehet backupi me te gjitha konfigurimet bazike.
6.	Sigurohemi qe te rimbyllim portat serish.
7.	Ringrejme firewalin e Miktorikut pas konfigurimeve.
8.	Konsultohemi me prodhuesin specialist te fushes qe sjell administratori ose shitesin e pajisjeve ne te cilat ka ndodhur incidenti.
9.	Trajnohet stafi me qellim mosperseritjen e incidentit.

Incidentet sic trajtohen ne rregulloren e AKEP, do ti njoftohen edhe AKEP sipas procedures ne rregullore dhe brenda afateve te percaktuara nga AKEP.

❖ MONITORIMI

Logimi dhe monitorimi

Pajisjet e mia eksportojne loget edhe jashte tyre dhe ketu perfshihen te gjitha ngjarjet emergjente dhe ato te gabimeve, te pajisjeve.

Monitorimi periodik i pajisjeve kryhet me qellim monitorimin punimit te pajisjes, deshtimeve te perkohshme apo me kohe te gjate, deshtimeve ne pjeset e pajisjeve, te trafikut si dhe te gjendjes se pajisjeve ne kohe reale.

Loget kontrollohen cdo mengjes nga punonjesi kryesor dhe nese vihen re incidente merren masa per eleminimin e ndonje demi ose nderhyrje.

Emergjencat

Te gjitha pajisjet dhe regjistri i klienteve behen backup ne menyre periodike nje here ne jave. Pajisjet rezerve jane parakonfiguruar dhe secila eshte bere prove dhe eshte testuar 4 here ne vit.

❖ **TESTIMI**

Testimi i Rrjetit dhe Sistemeve te Informacionit

Per cdo ndryshim qe kryhet, testojme rrejti per efektet qe ka dhene ndryshimi. Pershembull permendim ndryshimin e IPe dhe Klasave te IPve nga Albtelecom qe na furnizon me internet. Rrjeti testohet si dhe nxirren raporte nga sistemi i monitorimit. Sistemet e informacionit testohen si dhe i aplikohen praktikat me te mira per konfigurimin e pajsijeve dhe sistemeve nga ana e sigurise. Ndiqen ne menyre te vazhdueshme te gjitha perditesimet e prodhuesit me qellim permiresimin e sigurise.

❖ **AUDITIMI**

Vleresimet e Sigurise

Siguria vleresohet sipas skemes teknike te pajisjeve te rrjetit, akses fizik, ku ambientet jane te mbrojtura. Pajisjet e sistemit dhe rrjetit jane te mbrojtura nga fjalekalime te gjata e komplese dhe sistemet e operimit te pajisjeve jane te perditesuara me qellim garantimin e funksionimit te tyre.

Nga te gjitha pajisjet jane caktivizuar konfigurimet e panevojshme dhe qe rendojne funksionimin e tyre pa qene e nevojshme.

Per R&T sh.p.k.

Renis Tershana
Administrator