BLETA SHPK

PLANI I TRAJTIMIT
OSE REAGIMIT NDAJ INCIDENTEVE TË SIGURISË
DHE PLANI I VAZHDIMIT TË BIZNESIT
NË RASTET E SITUATAVE TË JASHTËZAKONSHME APO KATASTROFAVE

Baza ligjore

Pika 1 e nenit 6 të Rregullores Nr.37 datë 29.10.2015 "Mbi Masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike".

Detyrimet që burojnë nga Rregullorja 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", bëjnë që komopania jonë në fushën e komunikimeve elektronike të informojë Autoritetin e Komunikimeve Elektronike dhe Postare (AKEP) në rast se:

a) ndodh nje nga incidentet e meposhtme:

- *Mohimi i Sherbimeve Elektronike*
- *Kompromentimi i Sistemeve te Informacionit*
- *Manipulimi ose modifikimi i paautorizuar i të 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;

Lidhur me sigurinë, integritetin dhe mirëmbajtjen e funksioneve të rrjetit, kompania "Bleta" shpk ka përcaktuar polikat, objektivat dhe direktivat per te parandaluar problemet e lindura ne lidhje me sigurine e informacionit dhe te dhenave. Këto politika trajtojnë mbrojtjen e aseteve te kompanise dhe klientit duke trajtuar si aset cdo informacionin të klientit, cdo informacion te kompanise, cdo rrjet transmetimi te informacionit, cdo pajisje softwerike apo hardware-ike te Teknologjise se Informacionit, cdo sherbim te ofruar prej kompanise sidhe burimet njerezore te kompanise.

Objektivi i ketyre politikave eshte te minimizoje demet e biznesit duke parandaluar ndikimin e incidenteve te lidhura me sigurine e informacionit dhe te **dhenave mbi vazhdimesine e biznesit si dhe duke mbajtur ne kontroll risqet aktuale.**

Personi Pergjegjesi i Sigurise se Informacionit ne kompanine tone ka keto pergjegjesi:

1. Te siguroje qe proceset e nevojshme per Sistemin e Sigurise se Informacionit dhe te dhenave qe ato te themelohen, zbatohen dhe te mirembahen.

2. Te raportoje mbi performancen dhe nevojat per permiresim e Sistemit te Sigurise se Informacionit dhe te Dhenave.

3. Te promovoje ne kompani ndergjegjesimin per kerkesat e sigurise se informacionit dhe te Dhenave.

4. Te krijoje, identifikoje dhe te perditesoje Politiken e Sistemit te Sigurise se Informacionit dhe te Dhenave.

Eshte pergjegjesia e çdo punonjesi te kompanise te ndjeke Politiken e Sigurise se Informacionit dhe te Dhenave.

Politikat;

Informacioni dhe te dhenat, trajtohen si aset dhe konsiderohen si prone e kompanise. Punonjesit jane pergjegjes per mbrojtjen dhe trajtimin me kujdes te aseteve te kompanise.

Konfidencialiteti eshte nje vlere shume e rendesishme e kompanise. Te gjitha llojet e informacioneve dhe te dhenave, mbrohen me sisteme me standart te larta te sigurise.

Informacioni dhe te dhenat nuk mund te shperndahen pa autorizimi zoteruesit e informacionit dhe te dhenave.

Siguria dhe mbrojtjta e informacionit te klientit eshte shume e rendesishme per kompanine. Per kete qellim ne kontratat e nenshkruara me klientet eshte percaktuar qarte masatqe do merren

ne drejtim te dy paleve ne rast te shkeljes se kushteve te konfidencialitetit. Aktivitetet e jashteligjshme qe krijohen duke perdorur asetet dhe burimet e informacionit te kompanise nuk jane te pranueshme per kompanine.

Me poshte jane listuar disa nga aktivitetet te cilat jane te pa pranueshme nga kompania:

1. Demtimi i te dhenave

2. Perdorimi i informacionit dhe te dhenave per veprimtari te jashteligjshme

3. Shkaterrimi i pajisjeve, software-eve apo i çdo burimi informacioni

4. Vjedhja e pajisjeve, software-eve apo i çdo burimi informacioni

5. Perdorimi i burimeve te informacionit dhe te dhenave ne menyre jo korrekte duke shkaktuar humbje te performances se sistemeve te informacionit

6. Ofrimi i burimeve te informacionit paleve te treat apo kompanive konkurente

Keto aktivitete konsiderohen te jashteligjshme dhe cojne ne marrje te masave disiplinore sidhe proçedura respektive ligjore.

Incidentet e sigurise se informacionit dhe te dhenave, perpjekjet per aktivitete te jashteligjshme apo kanosjet te burimeve te informacionit duhet ti raportohen menjehere Personit Pergjegjes te Sigurise se Informacionit dhe te Dhenave.

Inventar per Riskun e Mbrojtjes se te Dhenave Personale

Nr. Risku

Emertimi i Riskut

Trajtimi dhe Plan veprimi

Nr.Mbrojtja e te dhenave personale

Veprimi identifikues

Opsionet e trajtimit

Veprimet e marra

Pergjegjes

Data e konstatimit

<u>MENAXHIMI I RISKUT</u>

Qellimi i kesaj politike eshte te siguroj kontroll te vazhdueshem sidhe te siguroj mbajtjen ne nivele te ulta te risqeve te Sigurise se Informacionit.

Personi pergjegjes per Menaxhimin e Riskut 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 Menaxhimin e Riskut eshte pergjegjes per:

- Identifikimin dhe raportimin e riskut ne menyre te pershtatshme drejt administratorit te kompanise, menaxhereve te tjere te kompanise, punonjesve te kompanise.

- Vleresimin dhe percaktimin e nivelit te riskut qe eshte i pranueshem dhe atij niveli i cili I kalon normat e mirefunksionimit te procesit, aktivitetit apo sherbimit.

- Ofrimin e informacionit per numrin e kercenimeve dhe nje informacion te detajuar mbi secilin prej tyre sebashku me nivelin e humbjeve qe ato shkaktojne.

- Organizimin e nje mbledhjeje periodike per informimin e kercenimeve ekzistuese sidhe masave te marra drejt kercenimeve te meparshme.

Personi pergjegjes per Menaxhimin e Riskut duhet te zbatoje nje procedure standarte per identifikimine e kercenimeve. Hapat qe duhet te ndiqen jane te listuara si me poshte:

- Analiza e Riskut e cila eshte procedura e pare ku aplikohet identifikimi i proceseve kur risqet e mundshme mund te iniciojne. Gjate kesaj faze kryhet edhe analiza per percaktimin e aseteve qe bejne pjese ne procedurat te cilat jane te zbuluara kundrejt ketij risku, kercenimet e ketyre aseteve, dobesimet e mundshme te tyre sidhe ndikimi ne teresine e sistemit nga ky kercenim.

- Vleresimi i Riskut i cili perfaqeson proceduren e nivelit te rezikut qe ky risk shfaq, periudhes kohore kur ky risk eshte i shfaqur sidhe frekuences se perseritjes se ketij risku.

- Trajtimi i Riskut i cili perfaqeson proceduren e veprimtatise se menaxhuesit te riskut per te ndaluar kete rist. Veprimtaria perbehet nga pikat e meposhtme:

 Vendosja ne kontroll e riskut.

 Minimizimi i riskut deri ne nivelet e pranueshme per sistemin.

 Eleminimi i riskut.

 Marrja e masave parandaluese per mos shfaqet e riskut te eleminuar.

Disa nga Risqet dhe kategorizimi i tyre eshte pershkruar si me poshte:

- Risqet nga burime njerezore:

 Publikim i Informacionit

 Kopje te informacionit jashte infrastrukturave te kompanise

 Vjedhje e informacionit

 Mos kryerje e detyrave specifike duke sabotuar sistemet

 Aktivitete joetike drejt aseteve te kompanise

- Risqe Natyrore:

 Zjarr

 Temperatura te larta apo te ulta

 Termete

 Permbytje

 Rrufe

 Lageshtire

- Risqe nga pa pergjegjshmeria:

 Viruse

 Humbje dokumentacioni

 Demtime te pavullnetshme te aseteve

 Gabime ne perdorimin e sistemeve

 Hedhje e materialeve te lengshme ne infrastriktura te ndrryshme.

SIGURIA E BURIMEVE NJEREZORE

Politikat e Burimeve Njerezore mbi sigurine, kontrollin, trajnimin si dhe trajtimin e shkeljeve

Qellimi i ketyre politikave eshte te siguroj nje kontroll te detajuar mbi personelin e kompanise.

Trajnimi i Kandidateve;

Zhvillimi i punonjesve permes trajnimit dhe edukimit te tyre mbi gjithe proceset dhe procedurat qe keta punonjes do kryejne ne kompani. Programet trajnuese jane dizenjuar per te zhvilluar aftesite e personelit ne kryerjen e pergjegjesive te percaktuara ne kompani. Nje element i programeve te trajnimit eshte dhe informimi I punonjesve mbi politikat e sigurise se informacionit sidhe politikat e trajtimit te shkeljeve apo akteve jashteligjore.

Aktiviteti i Punonjesit ne lidhje me Sigurine e Informacionit;

Gjate ushtrimit te pergjegjesive te percaktuara ne kompani punonjesi informohet mbi konfidencialitetin si nje ceshtje shume e rendesishme ne kompani.

SIGURIA E SISTEMEVE DHE PAJISJEVE

SIGURIA E RRJETEVE, SISTEMEVE DHE APLIKACIONEVE MBESHTETESE

Komapnia jone nderton, ofron dhe zhvillon nje rrjet te komunikimeve elektronike me fibra optike dhe rrjet wireless me disa akses pointe te deklaruara dhe te regjistruara ne AKEP. Rrjeti me fibra optike shtrihet ne zonen/zonat e Autorizimit dhe sa here te kemi ndryshime ne kete rrjet, ato do raportohen periodikisht ne AKEP sipas rregullores per Atlasin Elektronik.

Rrjeti me fibra optike suportohet me pajisje GPON te teknologjive te fundit ku pajisjet kryesore jane ato OLT dhe pajisjet ne terren jane ONU-te.

Per te marre internetin nga provideri ne perdorim nje ruter qendror i cili lidhet me pajisjen switch, pastaj me pajisjen OLT e cila ka kapacitet te zgjerueshem ne varesi te numrit te klienteve.

Gjithashtu cdo akses point ka nje tjeter ruter Mikrotik, per te rritur efektet e sigurise si dhe per ta aksesuar ne rruge te mbyllur. Pas paisjes switch vendoset nje paisje ruter Mikrotik Cloud Core per te ndare rrjetin tim nga provideri internet por edhe per te ndare ngarkesen ne rrjetin e fibres optike me rrjetin e akses pointeve.

Ruteri Mikrotik i akses pointeve ben menaxhimin dhe funksionimin me internet te antenave ne frekuencat e lira, dhe kontrollon kapacitetin e internetit te klienteve. Ky ruter eshte me IP reale.

Paisja Mikrotik instalohet ne panelin e paisjeve ne zyre dhe ka energji te vazhdueshme elektrike e garantuar me inverter me bateri qe mbajne deri ne 12 ore. Kulla eshte e garantuar me tokezim te mire per te mbrojtur pajisjet e mia nga shkarkimet atmosferike qe ne ate pike jane shume te shpeshta ne shume muaj te vitit.

Energjia stabilizohet me stabilizator tensioni per te perballuar ngarkesen elektrike qe konsumojne pajisjet ne rack.

Disa nga funksionet e pajisjeve ruterave qendrore Mikrotik jane:

1. Krijim rrjeti te qenderzuar i cili ofron besueshmerine e te dhenave dhe backup te sigurte

2. Implementim sigurie i te dhenave pavaresisht nga cila pike e rrjetit.

3. Percaktimi i te drejtave te nje perdoruesi , username dhe password per autentifikim.

4. Krijim lidhjesh private (VPN) mes pikash larg njera-tjetres, pavaresisht nga distanca mes tyre.

5. Segmentim i rrjetit te brendshem aty ku eshte e nevojshme

6. Realizimi i lundrimit te sigurt ne internet duke ngritur firewaalin e brendshem te tij i paraprogramuar me te gjitha mbrojtjet ndaj sulmeve drejt rrjetit.

Protokollet e punes dhe komunikimit te Mikrotikut jane te mbrojtura dhe te kriptuara, dhe garantojne:

1. Authentifikimin (Authentication)

2. Fshehtesine (Confidentiality)

3. Menaxhimin e celesave (Key Management)

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

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

Firewalli i Mikrotikut ndihmon ne filtrimin e trafikut ne internet, duke percaktuar rregulla strikte ndaj sulmeve dhe duke krijuar memorjen e nevojshme ne raste sulmesh, keshtu qe programe te demshme dhe hakere nuk kane asnje mundesi te kalojne Mikrotikun.

POLITIKAT E SIGURIMIT FIZIK, TE MJEDISIT DHE BURIMEVE

Qellimi i ketyre politikave eshte te siguroje parandalimin e rreziqeve qe perbejne asetet fizike, mjedisin e punes sidhe burimeve te ndrryshme.

Kjo politike aplikohet ndaj gjithe aseteve qe perbejne, jane pjese apo ndikojne ne shkembimin e informacionit ne kompani. Kjo politike mbulon gjithe ambientet e sistemeve te informacionit ku kompania kryen aktivitetin e saj.

Sigurimi Fizit i Aseteve te Kompanise;

Cdo aset i kompanise eshte i izoluar nga cdo akses fizik i jashtem.

Aksesimi i paautorizuar ne pajisjet e kompanise eshte parandaluar duke bllokuar dhe cdo lloj porte fizike apo virtuale. Te pa bllokuar jane vetem ato porta ku aksesi eshte i kontrolluar, enkriptuar dhe i mire izoluar nga kercenimet e jashtme.

Aksesi ne asetet e kompanise eshte gjithashtu i shkallezuar me nivele te ndrryshme te drejtash ne cdo pajisje si pjese e kompanise.

Siguria fizike eshte gjithashtu e kontrolluar nepermjet nje kompanie te kontraktuar per te ushtruar aktivitetin e saj. Kjo kompani mbulon sigurine e kompanise 24 ore ne te 7 ditet e javes. Thyerja e rregullave te sigurise fizike dhe aksesi i paautirizuar i nje punonjesi apo personi te jashtem ne ambjentet e vecuara te kompanise ben te mundur aktivizimin e sistemit te sigurise se kompanise kontraktuale dhe veprimin e menjehershem te saj.

Kontrolli i funksionalitetit te sistemit te sigurise fizike behet cdo muaj ku nje stimulim i thyerjes se sistemit kryhet per te matur kohen e pergjigjes. Gjithashtu gjate ketij stimulimi matet edhe riskun gjate periudhes se thyerjes se sistemit dhe kohes se pergigjes.

Sigurimi i Medisit nga Katastrofat Natyrore;

Cdo ambjet ne te cilin sistemet e informacionit jane te vendosura eshte implementuar sistemet e sigurise ndaj katastrofave natyrore.

Ne cdo ambjen eshte vendosur pajisjet e izolimit dhe ndalimit te zjarrit. Cdo system apo pajisje e sistemeve te informacionit eshte vendosur ne nje nivel mbi bazamentin fundor per te siguruar ruajtjen nga permbytjet apo lageshtia. Pajisjet e implementimit te sistemeve te informacionit jane izoluar hermetikisht per te mbllokuar rrezigjet e jashtme.

Siguria e Burimeve;

Politika e kompanise per sigurine e burimeve eshte qe cdo burim i cili siguron mbarevajtjen e sistemeve te informacionit te jete i garantuar ne vazhdueshmerine e tij nga sistemet e backup-it.

Sistemi i sigurimit te energjise elektrike per furnizimin e sistemeve te informacionit eshte i siguruar me nje system backup i perbere nga UPS (Furnizues i Panderprere i Energjise) i cili eshte gjate gjithe kohes aktive. Sistem Inverter dhe Baterish i cili hyn ne fuqi pas nderprerjes se energjise elektrike. Sidhe sistemi i furnizimit me energji elektrike me ane te gjeneratoreve elektrike ne rast te nje nderprerje te energjise eleketrike per nje periudhe disa orarshe.

Sistemi i Ftohjes per sistemet e informacionit eshte i aktivizuar ne cdo kohe dhe lidhet me sistemin e backup-it te energjise elektrike ne rast nderprerje te saj.

<u>POLITIKAT E KONTROLLIT TE AKSESIT</u>

Qellimi i kesaj politike eshte percaktimi i kerkesave mbi sigurine per te pasur nje akses te kontrolluar mbi burimet e informacionit.

Kjo politike aplikohet ndaj gjithe perdoruesve te aseteve te informacionit perfshire punonjesit e kompanise sidhe klientet te cilet perdorin pajisjet transmetuese te sherbimit te ofruar prej kompanise.

Kjo politike mbulon te gjitha ambientet e Sistemeve te Informacionit ku kompania operon.

Politika;

Kontrolli i aksesit eshte i nevojshem per sistemet pasi kane ne perberje te dhena sensitive dhe nevojiten te kene akses te kufizuar. Kjo politike pershkruan procedurat e perodurura per te kontrolluar akseset me qellim sigurimin e informacionit.

- Aksesi ne informacion duhet te jete i autorizuar ne menyre specifike.

- Aksesi ne informacion duhet te kontrollohet bazuar ne kerkesat e kompanise, dhe rregullave specifike te percaktuara per çdo sistem informacioni.

- Te gjithe punonjesit e kompanise duhet te aksesojne vetem ato asete dhe sisteme te informacionit te cilat jane te nevojshme per te permbushur detyrat e tyre te punes.

Te gjithe perdoruesit duhet te pajisen me nje deklarate me shkrim ose elektronike mbi te drejtat e aksesit te tyre, termat dhe kushteve per perdorimin e ketyre te drejtave.

Llogaria e perdoruesit duhet te rishikohet çdo 2 muaj per privilegjet e duhura.

Llogarite e perdoruesve te cilet largohen nga kompania duhet te hiqen menjehere mbas perfundimit te punes se tyre.

Te gjitha privilegjet e perdoruesve fillestar dhe ekzistues duhet te caktohen nepermjet nje autorizimi te Administratorit te kompanise.

Te gjithe perdoruesit duhet te zbatojne Politiken e Fjalekalimit.

Politika e Fjalekalimit perben krijimin e nje fjalekalimi komplekt ne te cilin perfshihen 4 lloje te ndrryshme kategorish te karaktereve sidhe nje gjateso jo me pak se 8 karaktere.

Te gjitha fjalekalimet qe i perkasin Administratorit te Sistemit i cili ka dhene doreheqje ose eshte pezulluar duhet te ndryshohen.

Kontrolli i aksesit te rrjetit;

Aksesi ne rrjete sherbime te rrjetit do te kontrollohet mbi bazen e kerkesave te sigurise dhe biznesit, dhe rregullave te kontrollit te aksesit te percaktuara per çdo rrjet.

Rrjetet e sistemeve te informacionit te kompanise duhet te ndahen ne segmente logjike bazuar ne nevojat e aksesit. Rrjeti i brendshem duhet te ndahet nga rrjeti i jashtem me kontrolle te ndryshme te sigurise rrethuese ne secilin prej rrjeteve. Lidhja ndermjet rrjeteve te brendshme dhe te jashtme duhet te kontrollohet.

Mekanizmat e duhur per kontrollin e rrugezimit duhet te implementohet per te kufizuar rrjedhen e informacionit ne rruget e rrjetit te percaktuar brenda kontrollit te kompanise. Kontrollet e rrugezimit te rrjetit duhet te bazohet ne burimet pozitive dhe mekanizmat e kontrollit te adreses se destinacionit.

Te gjitha sistemet e rendesishme dhe delikate si Router-at Kryesore qe Menaxhojne Rrjetin dhe Sistemi i Menaxhimit te Abonenteve duhet te kene nje arkitekture te mbyllur dhe shume te sigurt.

Monitorimi;

Te gjitha detajet e ngjarjeve lidhur me sistemin e informacionit duhet te logohen dhe ruhen per 1 muaj per sistemet e zakonshme dhe 2 muaj per sistemet kritike.

Te gjitha sistemet e informacionit dhe aplikacioni i biznesit duhet te monitorohet ndersa rezultatet e monitorimit duhet te rishikohen periodikisht. Te gjitha oret e sistemit duhet te sinkronizohen dhe rishikohen per pasaktesite dhe luhatje. Nje perpjekje e pasuksesshme login ne serverat kritik duhet te regjistrohet, investigohet, dhe pershkallezohet tek eprori i linjes se pare.

Menaxheri duhet te sigurojne monitorim te vazhdueshem dhe ne pajtueshmeri brenda kompanise.

POLITIKA E INTEGRITETIT TE SISTEMEVE DHE RRJETIT

Kjo politike garanton mbrojtjen e infrastruktures se sistemeve te informacionit nepermjet sistemit te antivirus-eve. Kjo politike pershkruan masat e ndermarra per te mbrojtur sistemet e kompanise nga viruset, Trojan-et, spyware, spamet, etj.

Kjo politike aplikohet ne te gjithe sistemet e informacionit te kompanise duke perfshire pajisjet e transmetimit, sistemet e IT sidhe sistemet e rendesise se vecante.

Personi pergjegjes analizon dhe shperndan perditesimet e mundshme te sistemeve te antiviruseve.

Politika;

Te gjitha sistemet e cenueshme nga sulmet e viruseve, malware, spam,etj. duhet te mbrohen nga software antivirus sa here te jete e nevojshme, perveç se kur lejohet nje perjashtim specifik dhe merren masa alternative per te garantuar te njejten shkalle mbrojtjeje.

Burime potenciale te viruseve perfshijne mjete te perbashketa si CD, USB, poste elektronike bllokohen dhe kontrollohen paraprakisht dhe me pas lejohen te punohet mbi to.

Te gjithe punonjesit qe perdorin pajisjet e kompanise duhet te perdorin gjate gjithe kohes disa praktika te cilat jane listuar si me poshte:

- Te tregojne kujdes kur hapin materialet bashkangjitur postes elektronike dhe ti kontrollojne per viruse perpara se ti hapin. Duhet te shtypin opsionin scan paraprakisht.

- Te tregojne kujdes kur hapin materiale nga mjete te tilla si USB ose CD. Duhet te shtypin opsionin scan paraprakisht.

- Te skanojne te gjitha mjetet e jashtme per viruse perpara se ti perdorin.

- Te njoftojne me email Personin pergjegjes te sistemeve te antiviruseve ne rast te nje sulmi nga virus-et.

- Punonjesit qe jane te autorizuar qe te lidhin kompjuteret e tyre me rrjetin e kompanise duhet te sigurohen se kompjuteret qe ata perdorin jane te mbrojtur nga viruset dhe perputhen me standardet e percaktuar ne kete politike.

Duhet te perditesohen sa here eshte e mundur ne baze te sistemit te antiviruseve cdo produkt qe kryen funksionin e nje antivirusi.

Personi pergjegjes per sistemet e antiviruseve duhet te mbedh log-et nga keto sisteme per te analizuar, identifikuar edhe eleminuar mundesi te tjera te mundshme te sulmeve nga antiviruset.

Duhet te aktivizohen ne cdo pajisje te punonjesve sistemet e sigurise se postes elektronike.

MENAXHIMI I OPERACIONEVE

Politikat e Menaxhimit te Operacioneve

Qellimi i kesaj politike eshte te percaktoje proceset operacionale per pajisjet dhe sistemet, si dhe ti mirembaj ato. Proceset e mirembajtjes mbulojne teresine e proceseve, veprimeve ose funksionimit ndaj te gjithe pajisjeve, sistemeve dhe sherbimeve te infrastruktures se rrjetit ne kompani. Keto politika sigurojne funksionimin e panderprere te te gjithe elementeve te rrjetit te kompanise.

Proceset

Keto politika ndahen ne disa kategori ne baze te hapave qe ndiqen per realizimin e nje operacioni:

- Planifikimi

- Implementimi

- Testimi

- Monitorimi

Planifikimi;

Planifikimi i nje operacioni do te thote krijimi i detajuar i instruksioneve te funksionimit te tij. Keto instruksione do te ndiqen perpikmerisht gjete hapave te implementimit dhe monitorimit. Krijimi i dokumentacionit te planifikimit duhet te jete i mire detajuar ne cdo aspekt teknike duke perfshire edhe lidhjen dhe ndikimin me operacine te tjera te tij.

Ne fazen e planifikimin dhe ne kalimin e metejshem te hapave te mesiper bejne pjese dy lloje operacionesh.Operacione te cilat jane pjese e nje sistemi apo sherbimi te ri te planifikuar per implementim. Sidhe operacione te cilat kan funksion mirembajtes, update-ues apo ndrryshues ne sistemet ose sherbimet ekzistuese te infrastruktures se rrjetit.

Implementimi;

Implementimi eshte faza ne te cilen versioni perfundimtar i planifikimit vihet ne zbatim. Gjate kesaj faze duhet te behen implementimet perkatese ne pajisjet apo sistemet qe bejne pjese ne kete operacion sidhe ne ato pajisje apo sisteme qe kane nje lidhje llogjike apo fizike me funksionimin e ketij operacioni por qe nuk jane pjese se tij.

Gjate fazes se implementimit duhet te merret parasysh numri i burimeve te nevojshme per kryerjen e saj sidhe periudha kohore gjate te ciles ky operacion do kryhet.

Implementuesi i ketij operacioni duhet te mari ne konsiderate kryerjen e tij gjate periudhes e cila ndikon me pak ose nuk ndikon ne performancen e asnje sherbimi apo nje sistemi.

Implementuesi i ketij operacioni duhet te dokumentoje cdo proces te kryer gjate operacionit sidhe vlerat e dhena ne konfigurimin perfundimtare ne rast kur ky process konsiston ne konfigurimin e nje pajisje apo sistemi.

Testimi;

Procesi i testimit konsiston ne matjen e parametrave te percaktuara gjate fazes se planifikimit. Vlerat e nxjerra nga matja e elementeve te operacionit te implementuar nuk duhet te jene te ndrryshme nga ato te percaktuara ne planifikim. Bejne perjashtim ato vlera te cilat ne fazen e planifikimit jane percaktuar me nje nivel ndrryshimi por duhet te jene brenda parametrave te lejuara te ndrryshimit.

Cdo proces testimi se bashku me vlerat e nxjerra prej tij duhet te dokumentohet.

Gjate ketij procesi duhet te stimulohen edhe incidentet e ndrryshme te percaktuara ne fazen e planifikimit dhe impakti i tyre ne nje pjese apo ne teresi te sistemeve dhe sherbimeve.

Procesi i testimit duhet te kryhet me shume se nje here sidhe duhet te kryhet gjate fazave te ndrryshme kohore gjate te cilit sistemi apo sherbimi ku ky operacion ben pjese ka sjellje apo vlera te ndrryshme.

Monitorimi;

Procesi i monitorimit eshte procesi me i rendesishem i fazes se menaxhimit te operacioneve. Pasi funksioni i ketij procesi eshte te kryej monitorimin dhe menaxhimin e operacionit i cili eshte pjese apo eshte ne teresi vete sherbimi ose sistemi I infrastruktures se rrjetit.

Monitorimi i proceseve kryhet ne dy menyra.

Menyra e pare eshte monitorimi i historise se funksionimit te procesit. Gjate ketij monitorimi personi pergjegjes kryen matje dhe analize mbi vlerat e meparshme te procesit nese ato jane brenda normave te percaktuara ne dokumentacionin perkates te operacionit.

Menyra e dyte eshte monitorimi ne kohe reale i procesit. Gjate ketij monitorimi personi pergjegjes merr ne konsiderate vlerat aktuale te procesit dhe i analizon ato duke i krahasuar me normat e parapercaktuara.

Te dy menyrat e monitorimeve te mesiperme mund te kryhen ne menyre te skeduluar ne varesi te kohes se percaktuar ne planifikimin e operacionit.

Gjate kesaj faze duhet te percaktohet dhe monitorohen edhe vlerat e burimeve te nevojshme per funksionimin e ketij operacioni te percaktuara ne fazen e planifikimit. Ne kete lloj monitorimi duhet te perdoren te dy menyrat e monitorimit.

Cdo vlere e regjistruar gjate fazes se monitorimit duhet te dokumentohet ne dokumentacionin perkates te operacionit apo sistemit te operimit.

Sistemet Operacionale te Backup;

Keto sisteme bejne pjese ne operacionet te cilet kryejne funksionin e tyre ne rast se cdo sistem apo sherbim nuk funksionin ose funksionimi i tij eshte jashte vlerave te lejuara.

Sistemet Operacionale te Backup duhet te jene te implementuara dhe te konfiguruara ne menyre qe ne rast mos funksionimi te sistemeve paresore sherbimet apo infrastruktura ne teresi e rrjetit te mos ndikoje nga mos funksionimi i nje pjese te tij.

Gjendja aktive e sistemeve operacionale te backup eshte ne varesi te cdo operacioni. Ne nje pjese te operacioneve eshte e nevojshme mos qendrimi aktive I ketyre sistemeve. Ndersa ne pjese te tjera operacionale eshte e nevojshme qendrimi i sistemeve operacionale te backup aktive.

Ne secilin nga operacionet ose funksionet e ndrryshme te sistemit ose sherbimeve duhet te jene te percaktuara dhe te dokumentuara sistemet operacionale te backup ne tre elementet perberes te tyre:

- Menyra e Funksionimit

- Vlerat e Funksionimit

- Koha e aktivizimit

Menyra e funksionimit percakton menyren se si sistemet operacionale te backup do kryejne funksionin e zevendesimit te sistemeve paresore.

Vlerat e funksionimit percaktojne vlerat te cilat sistemet e mesiperme do zevendesojne vlerat e sistemeve paresore.

Koha e aktivizimit percakton kohen e nevojshme te hyrjes ne funksion te sistemeve operacionale te backup nga momenti I nderprerjes se funksionimit te sistemeve paresore.

Per cdo sistem ose sherbim te infrastruktures se rrjetit te kompanise duhet te dokumentohen sistemet operacionale te backup dhe tre elementet e siperpermendur te tyre.

MENAXHIMI I INCIDENTEVE TE SIGURISE

Politikat e Menaxhimit te Incidenteve te Sigurise

Kjo politike kryen funksionin e raportimit dhe regjistrimit te incidenteve, vlerave jashte standarteve normale te funksionimit dhe masave te marra ne keto situata. Ne kete politike jane te perfshire te gjithe llojet e incidenteve qe lidhen me sistemet, pajisjet apo sherbimet e infrastruktures se rrjetit te kompanise.

Te gjithe punonjesit e kompanise duhet te raportojne dhe te informohen per cdo regjistrim incidenti qe ka ndikim ne procesin e punes se tyre.

Raportimi;

- Incidentet duhet ti komunikohen personit pergjegjes per regjistrimin e tyre.

- Duhet te zbatohen procedurat operacionale kur ky incident ndodh duke perfshire ekzaminimin, izolimin dhe masat e rikuperimit.

- Duhet te raportohen te gjithe procedurat e marra gjate procesit te ekzaminimit, izolimit dhe rikuperimit te sherbimin apo sistemit.

- Duhet te raportohen rezultatet e zgjidhjes se incidentit dhe vlerat e mbylljes se tij.

- Duhet te merren masa ndaj shkakut te ndodhjes se ketij incidenti perfshire burimet, proceset e punes apo individet.

- Identifikuesit e incidentit nese nuk jane personi pergjegjes i menaxhimit te incidenteve nuk duhet te nderhyjne ne riparimin e tij por duhet vetem te raportojne personin pergjegjes.

Me poshte jane te listuar kategorite ne te cilat incidentet grupohen:

- Nderprerje e sherbimit

- Difekte ne sistem apo sherbim

- Renie e cilesise se sherbimit

- Demtim hardware apo software i pajisjeve

- Vjedhje e pajisjeve

- Gabime njerezore

- Thyerje e sigurise

Nje grupin i rendesishem i incidenteve jane ato incidente te lidhura me cenueshmerine e sigurise se informacionit. Per kete arsye cdo punonjes i kompanise duhet te jete i vemendshem nda ndonje akti apo situate te cenuesshmerise se sigurise se informacionit duke raportuar menjehere tek personi pergjegjes.

Monitorimi;

Personi pergjegjes per menaxhimin e incidenteve duhet te jete ne gjendje jo vetem te identifikoj, regjistroj dhe analizoj nje incident por edhe te marri masa paraprake per identifikimin e incidenteve te ndrryshem. Per kete arsye duhet te kryhen monitorime apo te ngrihen sisteme

sigurie dhe alarmi ne menyre qe nje ngjarje e padeshiruar te identifikohet dhe te bllokohet pa kryer funksionin e saj.

Monitorimi duhet te kryhet per disa elemente thelbesore te sistemeve dhe sherbimeve te kompanise si:

- Funksionimi apo renia e sherbimeve ose sistemeve

- Sulme nga persona apo software te jashtem

- Aksese te pa kontrolluara ne sisteme apo pajisje

- Nderprerje e pa paralajmeruar e burimeve te ndrryshme

- Gabime njerezore ne operimin e sistemeve apo pajisjeve

Permiresimi;

Mbas zbulimit te shkakut te incidentit dhe marrjes se masave kundrejt tij duhet te zbatohen procedurat e permiresimit te operacioneve te ndikuara ne incident ne menyre qe te eleminohen raste te ngjashme ne te ardhmen. Disa nga procedurat qe duhet te zbatohen ne kete faze jane te listuara me poshte:

- Analiza e incidentit

- Identifikimi i shkakut te incidentit

- Izolimi i procesit, operacionit, sistemit apo pajisjet qe ka shkaktuar incident

- Planifikim i masave parandaluese ne raste te tilla te ngjashme

- Analize e rekordeve per incidente te ngjashme per te marre masat e duhura ne parandalimin e tij . Raportimi i Incidenteve do te kryhet ne nje sistem rekordesh sipas skemes se meposhtme dhe duhet te perditesohet nga personi pergjegjes i menaxhimit te incidenteve.

MENAXHIMI I VAZHDIMIT TE BIZNESIT

Politikat e vazhduesshmerise se sistemeve dhe sherbimeve

Qellimi i ketyre politikave eshte te krijojne nje procedure operacionale per te lejuar vazhdueshmerine e sistemeve dhe sherbimeve ne raste incidentesh apo katastrofe natyrore.

Me marrjen e masave dhe kryerjen e procedurave operacionale do te bej te mundur qe kompania te:

- Vazhdoj ofromin e sherbimit.

- Vazhdoj ruajtjen e informacionit te kompanise dhe klienteve te saj

- Venien ne fuqi te sistemeve operacionale te backup

- Kete humje minimale ne sherbim dhe funksionin te proceseve

- Ndaloj ndikimin e tyre ne mireqenien e punonjesve apo klienteve te kompanise

Aplikimi

Me poshte eshte diagrama e hapave qe merren ne rastin e nje incidenti apo katastrofe natyrore:

Operacione Standarte

Incidet apo Fatkeqesi Natyrore

Izolim i Procesit te Perfshire

Ngritja e Sistemeve Operacionale te Backup

Rikuperim I Procesit

Implementim I Operacioneve Standarte

Informimi;

Duhet te behet e mundur dallimi i katastrofes apo incidentit duke i kategorizuar ato. Ne kete menyre per cdo kategori te meren masat dhe aksionet perkatese per evitimin, izolimin dhe eleminimin e tyre. Kategorite jane si me poshte:

- Natyrore

 Zjarr Termet Permbytje

- Njerezore

 Shperthim Kimike Difekt ne proces pune Vjedhje Humbje

- Infrastrukture Sisteme te ndaluara Energji e nderprere Humbje komunikimi Ftohje/Ngrohje jashte normave te lejuara

- Teknologji Informacioni Sulme Cybernetike Demtim Hardware Kodim I gabuar Humbje te dhenash Demtim Software Gabime Njerezore

Veprimet e Rikuperimit

Elementi me i rendesishem i menaxhimit te situatave te emergjences eshte koha e pergjigjes ndaj situatave te tilla. Per kete arsye duhet te kategorizihet lloji I situates se emergjences dhe koha e pergjigjes respektive.

Niveli i Prioritetit;

Pershkrimi i Sistemit apo sherbimit

Koha e Pergjigjes, Kritike

-Sistemi apo Sherbimi eshte jo aktive

-Pjese kritike te Sistemit apo Sherbimit nuk eshte funksional

-Veprimtari jashte standartit te Sistemit apo Sherbimit

-Humbje e te Dhenave sensitive te kompanise

0-6 Ore, I Larte

-Pjese te rendesishme te Sistemit apo Sherbimit nuk jane funksional

-Aksese te pjesshme ne Sisteme apo Sherbime nuk jane aktive

7-14 Ore, Mesatar

-Sistemet apo Sherbimet jane duhe funksionuar por nje pjese e vogel e tyre nuk funksionin brenda standarteve

-Instalime te ndrryshme kane pasur incidente minimale

15-24 Ore, I Ulet

-Probleme minimale qe nuk ndikojne ne funksionalitetin e punes

-Probleme minimale qe nuk ndikojne ne ofrimin e sherbimit

24-72 Ore

POLITIKAT E LOGIMIT

Qellimi i kesaj politike eshte te menaxhor sistemin e ruajtjes dhe perdorimit te logeve te gjeneruara gjate gjithe aktiviteteve te sistemeve ose sherbimeve kryesore ne infrastrukturen e rrjetit te kompanise. Te dhenat e logeve permbajne informacion te detajuar te aktiviteteve mbi pajisjet, aplikacionet, sistemet dhe sherbimet qe bejne pjese ne infrastrukturen e rrjetit.

Pajisjet e rrjetit duke perfshire router, akses point apo switch mund te gjenerojne informacione prej logeve duke informuar administratorin e rrjetit mbi aktivitetet e kryera ne keto pajisje.

Aplikacionet mund te identifikojne veprimet e kryera ne to, kohen e kryerjes dhe qellimin prej logeve te regjistruara.

Sistemet apo sherbimet jane te kategorizuar ne elemente te infrastruktures se rrjetit te cilat do implementohet sistemi i regjistrimit te logeve per aktivitet qe kryhen ne to.

Duke menaxhuar sistemet e logeve perfitohet shume informacione te rendesishme per sigurine, performance dhe menaxhimin e burimeve te ndrryshme te sistemeve apo sherbimeve te rrjetit. Disa nga keto informacione kategorizohen si me poshte:

- Aksesi. Perdoruesi i cili ka aksesuar nje pajisje apo sistem te rrjetit.

- Ndrryshimi. Parametrat e ndrryshuara ne nje pajisje apo sistem te rrjetit.

- Siguria. Veprimtari te ndrryshme ne elementet e infrastruktures qe cenojne sigurine e sistemeve apo sherbimeve.

- Sherbimet e ofruara. Kategorizim, ndrryshim apo modifikim i sherbimeve te ofruara.

- Problematikat. Probleme ne funksionimin brenda parametrave te elementeve te infrastruktures se rrjetit.

- Perdorim i Burimeve. Analize e perdorimit te burimeve te ndrryshme ne sistemet e rrjetit.

- Aktivitet Standarte. Aktivitetet standarte brenda operacioneve te lejuara nga ana e perdoruesve te ketyre pajisjeve, sistemeve apo sherbimeve.

Administratori i rrjetit eshte pergjegjes per menaxhimin e sistemeve te logeve per elementet e percaktuar te infrastruktures se rrjetit.

Loget e Pajisjeve te Rrjetit

Ne kete kategori bejen pjese ato pajisje qe perbejne infrastrukturen e rrjetit te komanise:

- Router

- Access Point

- Switch

- Firewall

Informacionet qe mund te gjenerohen nga keto sisteme log-esh jane te ndrryshme por perqendrimi eshte fokusuar ne disa prej tyre:

- IP Address te pikave fundore te rrjetit

- Parametrat teknike te rrjetit per aktivitetin e nje pajisje apo klienti

- Sherbimi i kryer

- Ora dhe Data e aktiviteteve

- Vlerat e trafikut te gjeneruar

- Veprimtaria e marre nga pajisja per kerkesat e mesiperme

Loget e Sistemeve dhe Sherbimeve

Ne kete kategori bejne pjese ato pajisje qe operojne per nje sistem te caktuar apo per te ofruar nje sherbim te caktuar. Atom und te karakterizohen si me poshte:

- Sisteme Operacionale

- DNS Server

- Web Hosting Server

- Virtual Server

- Radius Hosting Server

Informacionet qe mund te gjenerohen nga keto sisteme log-esh jane te kategorizuara si me poshte:

- Kerkese per aksesim

- Kerkese per veprim

- Ora dhe Data e aktiviteteve

- Veprimtaria e marre nga perdoruesit e ketyre sistemeve apo sherbimeve

- Parametrat e ndrryshimeve te kryera

Loget e Aplikacioneve

Ne kete kategori bejne pjese ato aplikacione te cilat ofrojne nje sherbim te rendesishem ne infrastrukturen e kompanise.

- Radius Server

- Aplikacioni Financiar

Informacionet qe mund te gjenerohen nga keto sistem log-esh jane te kategorizuara si me poshte:

- Operacionet e kryera ne to

- Ndrryshimet ne kategorite e sherbimeve te ofruara

- Ora dhe Data e aktiviteteve

- Veprimtaria e marre nga perdoruesi

- Informacion mbi aktivitetin e klienteve te regjistruar

Keto informacione mund te perdoren ne menyre te vazhduar nga cdo punonjes I kompanise per te mbarevajtur detyrat e percaktuara por kjo kerkese duhet te jete e shoqeruar me autorizimin e Administratorit te kompanise per informacionin e kerkuar.

Keto informacione mund te perdoren nga Administratori i Rrjetit per te analizuar veprimtarite e meparshme nga sistemet, pajisjet apo sherbimet per vlerat e trafikut te gjeneruar, vlerat e burimeve te perdorura apo veprimtari te tjera qe kane ndikim ne administrimin e rrjetit.

Keto informacione mund te 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 ruajne te dhena deri ne nje muaj nga momenti i regjistrimit te logeve ne sistem.