NETSYSCOM Sh.p.k
netsyscom.al@gmail.com

Tirane me 19.07.2019

Lenda: Dergohen masat e marra nga kompania NETSYSCOM Sh.p.k per sigurine e rrjetit dhe sherbimeve.

Autoritetit te Komunikimeve Elektronike dhe Postare

Te nderuar

Ne zbatim te Rregullores nr. 37 te AKEP dhe kerkesave te AKEP per sigurine e rrjetit, ju dergojme masat e marra nga kompania NETSYSCOM Sh.p.k per sigurine e rrjetit dhe sherbimeve.

Me respekt

Administratori

Dede Bukaqeja

1.Qeverisja dhe Menaxhimi i Riskut

NETSYSCOM Sh.p.k ka bere te mundur te gjitha masave te arsyeshme, te pershtatshme, praktike dhe efektive te sigurise, per te mbrojtur progeset e rendesishme dhe aktivetin per arritjen e objektivit te sigurise.

Qellimi yne ne teresi eshte te:

1.Strukturojme dhe mirembajme pozicionin tone si nje partner i besuar per klientet e mundshem dhe autoritetet qe kane nevoje te aksesojne te dhenat e NETSYSCOM Sh.p.k
2.Sigurojme qe te gjitha sherbimet tona ofrohen me standardet me te larta teknike dhe me etiken e duhur;
2.Mbrojme informacionin qe ruhet ne sistemet IT te NETSYSCOM (te dhena financiare dhe te klienteve).
3.Implementojme nje politike te sigurise se informacionit qe te ruajme nje sherbim te panderprere ne 99% te kohes.
4.Sigurojme vazhdimesi te biznesit dhe minimizojme demet e biznesit duke parandaluar dhe minimizuar impaktin e incidenteve te sigurise.
5.Ruajme rreziqet ekzistuese ne nivelet aktuale.

Per te na ndihmuar qe te arrijme keto qellime, ne kemi implementuar nje politke te Menaxhimit te Sigurise se Informacionit. Politika ka disa elemente te saj sic jane survejimi me anen e programeve te kontrollit, analizimi i trafikut dhe kapacitetve, monitorimi i portave te sigurise, etj. Struktura e kesaj poltike implementuar duke perdorur nje nderthurje objektivash dhe dokumentim progesesh. Grupi yne i menaxhimit ne NETSYSCOM Sh.p.k eshte i angazhuar te bashkepunoje ngushte me stafin tone per te zhvilluar dhe permiresuar kete sistem. Si pjese te ketij angazhimi, ne:

Perdorim trajnimin dhe komunikimin me te gjithe punonjesit per tu siguruar qe kjo politike eshte kuptuar dhe vene ne veprim;
1.Vendosim poltiken e Menaxhimit te Sigurise se Informacionit ne kulturen dhe praktikat e perditshme te Netsyscom shpk, si nje angazhim afatgjate per permiresimin e vazhdueshem te sigurise se informacionit

2.Sigurojme qe informacioni yne menaxhohet shume mire, duke permbushur tre parimet e sigurise se informacionit: te konfidencialitetit, integritetit dhe

disponueshmerise.
3.Sigurojme disponueshmerine e burimeve te nevojshme ne NETSYSCOM Sh.p.k per te mirembajtur nen kontroll Sigurine e Informacionit.
4.Sigurojme qe kontrollet e pershtatshme per sigurine e informacionit jane active.
5.Sigurojme qe rreziqet e reja dhe te ndryshueshme, menaxhohen ne menyren e duhur dhe profesionale.
6.Sigurojme qe ne i kuptojme dhe jemi ne perputhje me rregulloret e AKEP dhe KMDPDI dhe kerkesat ligjore qe prekin aktivitetin e punes tone.
7.Politika e Menaxhimit te Sigurise se Informacionit rishqyrtohet ne takimet e grupeve te punes ne terren, per te siguruar qe politika vazhdon te jete efektive dhe e aplikueshme pervec sistemit tone teknik, edhe ne pjese te tjera te rrjetit dhe tek klienti fundor, duke e pare nga kendveshtrimi i permiresimit te vazhdueshem te tij.

TAB EL A PER VLERESIMIN E IMPAK TIT TE INCIDENTIT TE SKil RISE

Kohezgjatja e incidentit te sigurise(nderprerjes sc sherbimit, interceptimit te komunikimeve, software te dcnishcm,, moditlkiini i te (1 henave)	*Me teper se 1 ore, por me pak se 2 ore*	*Me teper se 2 ore*
Nuniri i perdoruesve te prekur nga incidcnti ose % e tyre ndaj numrit total te perdoruesve te ofruesit		
>1000 ose >5%	*Mesatar*	*I Larte*
Ne rast te nje numri te panjohur te perdoruesve te prekur nga incidcnti i sigurise, zona gjeografike e slitrirjes se incidentit te sigurise		
>20 ore	*Mesatar*	*I Larte*
Vleresimi Perfundimtar i Impaktit:	*Mesatar*	*I Larte*

2.Siguria e Burimeve Njerzore

Cdo punonjes i NETSYSCOM Sh.p.k ka pergjegjesite e tij ne lidhje me sigurine. Pergjegjesia per sigurine percaktohet qe ne fazen e marrjes ne pune dhe perfshihet ne manualet e vendeve te punes dhe ne kontratat e punesimit.

Menaxheri i shoqerise sone, siguron qe ne pershkrimin e detyres, te adresohen ceshtjet e sigurise qe lidhen me te.

Rolet dhe pergjegjesite qe lidhen me sigurine, perfshihen ne pershkrimet e vendeve te punes. Kjo siguron pergjegjesine e te gjithe punonjesve. Pershkrimet e vendeve te punes perfshijne si pergjegjesite qe kane te bejne me zbatimin ose me mirembajtjen e rregullave te pergjithshme te sigurise, ashtu dhe ato specifike per mbrojtjen e aseteve te veganta ose per ekzekutimin e proceseve te vecanta.

Te gjitha aplikimet per punesim shqyrtohen me kujdes nga pikepamja e sigurise. Te gjitha pranimet e reja ne pune ne NETSYSCOM behen ne perputhje me rregullat e dokumentuara, duke i trajtuar aplikantet te barabarte, pa diskriminim dhe pa nderhyrje miqesie.
Ne te gjitha kontratat e pranimit ne pune, perfshihet nje deklarate ku punonjesit e rinj duhet te pranojne me shkrim, se bihen plotesisht dakort me kerkesat e NETSYSCOM Sh.p.k mbi:

- konfidencialitetin
- sigurine e informacionit
- te dhenave personale.

Administratori rrjetit ne NETSYSCOM Sh.p.k eshte pergjegjes per sigurine e rrjetit dhe mbikqyrjen e vazhdueshme te saj.

Ai u garanton punonjesve te rinj te strukturave perkatese te NETSYSCOM Sh.p.k qe u eshte dhene niveli i duhur i aksesimit ne pajisjet dhe ne sistemet e kompanise perfshi ketu llogarite e perdoruesve per kompjuterat, miratimin e lejes se aksesimit te sistemeve, te dhomave te serverave, te nyjeve te rrjetit, etj.

Te gjitha aplikimet qe behen per dhenien e te drejtes se aksesimit ne sistemet kompjuterike te kompanise, (perfshi ketu llogarine personale fillestare per pjesetaret e rinj te personelit dhe gdo ndryshim ne vazhdim ne te drejtat per aksesimin e

sistemeve) behen me shkrim, duke perdorur nje formular standard, i cili firmoset nga Administratori i rrjetit i cili g'ithashtu e mbikqyr perdorimin e te drejtes per akses ne sistem.

Te gjithe pjesetareve te rinj u jepen instruksione te plota per procedurat e teknolog'ise se informacionit dhe ne veganti per kerkesat ne lidhje me geshtjet e sigurise. Keto instruksione duhet te perfshijne te pakten:

1. Perdorimin e pergjithshem te mjeteve te teknolog'ise se informacionit.
2. Ndihmen e kualifikuar IT helpdesk.
3. Familiarizimin me politiken e Sigurise se kompanise e rregullat e sigurise.
4. Trajtimin me kujdes te informacioneve konfidenciale
5. Politiken e perdorimit te internetit, te emailit etj ne kompanine NETSYSCOM Sh.p.k.
6. Rregullat per fjalekalimet.

Kjo behet para se atyre t'u hapet ndonje llogari perdoruesi ose t'u jepen privilegje per te aksesuar sistemet e NETSYSCOM Sh.p.k.

Menaxheri i NETSYSCOM Sh.p.k eshte pergjegjes per te garantuar zbatimin e procedurave te sigurise ne rastet kur pjesetare te personelit te tyre largohen nga puna.

Eshte pergjegjesi e Menaxhierit te Netsyscom shpk te siguroje, qe kur nje pjesetar i personelit largohet nga puna, t'i hiqen te githa te drejtat e aksesimit dhe t'i kerkohet te dorezoje te githa kartat e aksesimit, gelsat, shenimet, kompjuterat, etj te cilat i ka patur ne perdorim.

Procedurat e teknologjise se informacionit per mbylljen e llogarise se perdoruesit dhe per heqjen e te drejtave te aksesimit te sistemit teknik te NETSYSCOM Sh.p.k, behen para se pjesetari i stafit te largohet fizikisht nga ambienti i punes.

Personi pergjegjes i caktuar nga per administrimin e rrjetit dhe sistemit te NETSYSCOM Sh.p.k, informohet menjehere kur ndonje pjesetar i personelit e le punen ose afati i tij i punesimit mbaron per cdo lloj arsyeje.Eshte pergjegjesi e Menaxherit te NETSYSCOM Sh.p.k te siguroje qe kjo gje u krye sa me pare. Punonjesit te cileve u nderpriten marredheniet e punes, u kerkohet te largohen nga Kompania menjehere. Ndersa punonjesit, te cilet kane kerkuar vullnetarisht largimin e tyre per aresye te ndryshme, mund te vazhdojne punen normalisht edhe per nje periudhe mbasi ata te kene kerkuar largimin. Njoftimi tek Administratori i

NETSYSCOM Sh.p.k per largimin nga puna te nje personi te caktuar, duhet te permbaje udhezimet per korrektimin e te drejtave te perdoruesit te personit qe do te largohet.

3. Siguria e Sistemeve dhe pajisjeve

NETSYSCOM Sh.p.k ka nje sistem te kompletuar, persa i perket sherbimeve te informacionit dhe ofrimit te sherbimit internet.
Baza e ketij sistemi jane Ruterat, serverat dhe rrjeti. Me anen e Ruterit kryesor Cisco Secure Ruter, NETSYSCOM Sh.p.k ka arritur te kombinoje sigurine, hyrjen ne Internet, lidhjet VPN, dhe rrjetin e shtrire deri tek klienti, te menaxhuar ne nje router te vetem qe eshte i lehte per tu perdorur.

Routeri Cisco Secure ofron:

a) Siguri te avancuar: Mbron rrjetin e NETSYSCOM Sh.p.k nga sulmet dhe viruset.
b) Hyrje VPN: Hyrje e sigurt dhe e larget dhe lidhje pike me pike.
c) Rrjete te sigurta opsionale wireless: Mbajini punonjesit tuaj te lidhur edhe kur jane larg tavolines se tyre.
d) Cilesi e sherbimit: Ofron lidhje te rrjedhshme zeri dhe video

Cisco Secure Router i NETSYSCOM Sh.p.k i kombinuar me pajisjet rutera Mikrotik, bejne izolimin perfekt te sistemit teknik, duke e bere ate mjaft te sigurte ndaj sulmeve dhe viruseve.

Pervec elementeve te Firewall, ruterat Mikrotik ofrojne edhe:

- Siguri e forte: Ule rreziqet e biznesit te lidhura me viruset dhe kercenime te tjera te sigurise.
- Sherbime bashkevepruese me shpejtesi broadband: Merret maksimumin i sigurise ne nje lidhje broadband.

  VPN: teknologjia Virtual Private Network lejon punonjesit e larget te NETSYSCOM Sh.p.k ose te kompanive ne rrjetin e NETSYSCOM Sh.p.k ,te lidhen me rrjetin nepermjet nje rruge te sigurte Interneti. Ata mund te hyjne ne e-mailet dhe dosjet e tyre si te ishin ne zyrat e tyre.

- Siguria: Firewall te ndertuara perbrenda ne sistemin e tij operativ dhe nje

enkriptim i avancuar, dhe autentifikimi i karakteristikave ne Mikrotik, e mbron rrjetin e NETSYSCOM Sh.p.k nga kercenimet e jashtme, duke mbajtur asetet e biznesit te sigurta.

- Lidhja: Te githe Routerat vijne me disa lidhje opsionale per zgjerim maksimal te rrjetit. Kur perdoren per nje numer te rritur fizik te portave fizike te lidhjeve ne rrjet ose lidhjeve wireless, keto routera jane ndertuar per te derguar ndarje lidhjesh te avancuara.

Levizshmeri e sigurt: Pjeset e rrjetit wireless aksesojne me me shume siguri dhe me shpejtesi me te larte, qe lejon punonjesit e nje klienti biznes te kene rrjet te tyre me te sigurt.

Jane disa pika kyce qe meren ne Konsiderate per sigurine e sistemit per te ndaluar aksesin e paautorizuar ne sistemin tone:

I. **Perdorim password te forte.** Nje nga menyrat me te mira qe te jemi te sigurte eshte perdorimi I passwordeve te forte.Use strong passwords. Nje sulem i forte eshte kur sulmuesi perdor nje system te automatizuar per te patur passwordet sa me shpejt te jete e mundur. Passwordet qe permbajne karaktere dhe hapesira, duke perdorut te duja shkronjat kapitale ose te vogla, me mire se sa perdorimi i numrave, eshte me e veshtire se sa perdorimi i fjaleve te zakonshme, emir juaj apo ndonje personi te afert apo ditelindjen tuaj.kujtoni se sa me shume rritet gjatesia e fjalekalimit tuaj rritet dhe numri I pergjithshem I mundesive qe mund te perdoren. Ne pergjithesi , cdogje me pak se 8 karaktere eshte me i lehte per tu vjedhur nga sulmuesit. 12, ose 16 eshte mire. Por jo dhe gjume te gjate dhe te veshtire per tu mbajtur mend.

II. **Nje mbrojtje e mire e perimetrit perreth.** Jo te gjitha sigurite ndodhin ne desktop. Eshte nje ide e mire te perdorni nje mur mbrojtes te jashtem firewall/ router qe te mbroje kompjuterin tuaj edhe nqs keni vetem nje kompjuter. Ose ju mund te porositni nje pasije router Linksys, D-Link, ose ne nivele me te larta ju mund te menaxhoni switche , routers , firewalls nga vete kompanite. Proxy servers, antiviruset gateways dhe filtrimet e spameve jane nje menyre e mire sigurie .

III. **Update (azhornim) software-in .** Kur shqetesime te tilla si testimi i

patch-eve mund te jete ne nje situate kritike per shume arsye, mos azhornimi per sigurine mund te jete e rrezikshme nga sulmuesit per kompjuterin tuaj Mos lejoni qe programet qe keni te instaluar te kalojn nje kohe skedulimi te gjate pa update.

IV. **I fikim sherbimet qe nuk perdorni me.** Shpesh , perdoruesit nuk e dine se cfar sherbimesh jane duke ekzekutuar ne sistemin e tyre. Telnet dhe FTP duhen te mbyllen (fiken) ne kompjuter kur nuk jane me te nevojshme. Sigurohuni qe te jeni ne dijeni te cdo sherbimi qe po perdorni ne kompjuterin tuaj

V. **Enkriptimi i te dhenave tona.** Nivele te ndryshme te enkriptimit te te dhenave jane vlefshme ne sigurine e kopmjuterave te perdoruesit apo te administratorve. Te vendosesh llojin e enkriptimit qe ju duhet varet nga rrethanat. Enkriptimi I te dhenave mund te mbuloje nje rreze qe nga perdorimi i mjeteve kriptografike per file- pas -file deri ne nje system file-sh enkriptimideri ne nje disku enkriptimi plot(Full disc encryption). Por kjo nuk mbulon particionet e boot-imit, pasi do te kete nevoje per nje support deshifrimi nga hardware te specializuar, por ju nese doni privaci ia vlejne shpenzimet.

VI. **Mbroni te dhenat tona me backup**. Nje nga menyrat me te rendesishme te mbrojtjes esht te besh backup te dhenave tuaja. Strategjite per tepricen e te dhenave mbulojne nje rreze nga dicka e thjeshte ruajtja ne CD deri te backup periodik te automatizuar te serverit.

VII. **Enkriptoni komunikimin e ndjeshem.** Sistemet kriptografike per mbrojtjen e komunikimit gjenden kudo. Programet suportojne PGP per email, Off Record per plug-ins per klientet IM , tynelet e enkriptuara per te mbajtur komunikimin e qendrueshem duke perdorur protokollet e sigurt si SSH dhe SSL ose shume mjete te tjera per sigurine.

VIII. **Nuk i besojme rrjeteve qe nuk i njohim (huaja).** Kjo eshte vecanerisht per rrjetet wireless. Nuk ka asgj te keqe perdorimi I rrjetit wireless ne nje local por e rendesishme eshte te keni siguri per sistemin tuaj. Per shembull eshte me kritike qe ju te mbroni komunikimin me enkriptim nje nje rrjet te hapur wireless duke perfshire ketu dhe kur lidheni me web site kur ju perdorni nje seksion login ose kur fusni nje username dhe password. Kontrolloni sistemin tuaj ne te duja anet jashte/ Brenda per te pare se cfar mundesish kane keqberesit te sulmojne dhe per ti ndaluar ato.

IX. **Keni nje Ushqyes te panderpreshem.** Perdorimi I UPS nuk perdoret vetem per te mos humbur te dhenat kur nderpritet energjia, UPS ndihmon jut e mbroni si pjesen hardware dhe te dhenat tuaja

X. **Monitoroni sistemin per threats dhe nderhyrje te tjera.** Jo vetem perdorimi i kesaj liste per sigurine e sistemin tuaj mund te mbroje nga

nderhyrje e keqija, Duhen dhe mjete monitoruese. Monitorimi I rrejtit ose teknika te tjera monitorimi do te mbronin punen tuaj dhe aksesin e paautorizuar.

Ruterat Mikrotikut garantojne qe protokollet e punes dhe komunikimit jane te mbrojtura dhe te kriptuara, duke perfshire:

1) Authentifikimin.
2) Fshehtesine.
3) Menaxhimin e celesave te sigurise se informacionit

Authentifikimi/logimi i cdo useri ne Miktorik kryhet permes kodit HMAC (Hash based Message Authentication Code) me username dhe password personal.

Siguria e Serverave

Gjatë hapjes së një adrese elektronike, regjistrimit në një website,
shkarkimit të një materiali apo kryerjes së një transaksioni online, shpesh ndeshemi me kërkesën për të shpjeguar natyrën e një teksti të paraqitur në trajtë të shtrembëruar. Një masë e tillë zbatohet me qëllim që të parandalojë regjistrimet automatike dhe parimi në të cilin bështetet funksionimi me sukses i saj , konsiston në faktin që asnjë program kompjuterik, sado i sofistikuar që të jetë, nuk mundet që të lexojë një tekst të shtrembëruar sikurse mund të bëhet nga njerëzit nëpërmjet përdorimit të shqisave të tyre të shikimit.

Modeli i testit CAPTCHA të bazuar në paraqitjen e teksteve të shkruara për të bërë dallimin midis individëve përdorues dhe kompjuterave është modeli i parë i zhvilluar në këtë drejtim. Ndërkohë, në vijim janë përpunuar edhe modele testesh të tjera të cilat sipas rastit, përveç verifikimit të përdoruesve në sajë të aftësisë së tyre për të parë dhe kuptuar një tekst të shkruar kanë përfshirë edhe forma verifikimi akoma më komplekse që kërkojnë domodoshmërisht edhe aftësi të menduari mbi subjektin e dhënë.

Testet Audio

Ndërtimi i testeve automatike për dallimin e njerëzve nga kompjuterat mund të bazohet edhe në përdorimin e efekteve zanore. Në një rast të tillë, programi pasi përzgjedh rastësisht një fjalë apo seri numrash, e ndërvendos atë në një regjistrim zanor, i cili vështirëson dëgjimin e fjalëve apo numrave të shprehur për shkak se në

të përmbahen edhe efekte të tjera zanore si tinguj apo zhurma të ndryshme. Më pas përdoruesit i kërkohet që të shkruajë përmbajtjen e shprehjes së dëgjuar në regjistrim.

Zbatimi i testit CAPTCHA, funksionon më së miri për sprapsjen e rrezikut që vjen nga sulme të tilla pasi duke qenë se ato bazohen në kërkesa të dërguara në mënyrë automatike nga kompjutera të kontrolluar nga sulmuesi, nuk mundet që të kalohet pengesa për dallimin e tekstit të paraqitur sepse ky veprim është i lidhur në mënyrë të pashmangshme me aktivitetin njerëzor

<u>Aksesi dhe siguria e aseteve te NETSYSCOM Sh.p.k:</u>

1. Te githa pajisjet ne pronesi te NETSYSCOM Sh.p.k dhe te githa pajisjet e tjera kritike mbrohen fizikisht nga kercenimet e sigurise dhe nga rreziqet e mjedisit. Te githe serverat dhe pajisjet e komunikimit (domethene routerat, switch-et, firewallet, etj jane te vendosura ne ambjente jane te vendosura ne ambjente vetem per personelin e autorizuar nga Administratori i kompanise NETSYSCOM Sh.p.k.
2. Hyrja ne dhomen e serverave dhe pajisjeve te sistemit, behet neprmjet nje sistemi aksesi me karte qe siguron identifikimin e personit qe hyn ne sistem, daten, oren dhe sa here ka hyre dhe dale. Karte aksesi kane vetem 3 persona, Pergegesi i Sistemit dhe Rrjetit, Menaxheri i kompanise NETSYSCOM Sh.p.k dhe Administratori i kompanise NETSYSCOM Sh.p.k.
3. Te githa aksesimet ne asetet e NETSYSCOM Sh.p.k dhomen e serverave dhe ne nyjet e rrjetit jane te kontrolluara dhe mbahen log-e ku shenohet emri i personit ose i personave, arsyet e hyrjes, data/ora dhe veprimet e kryera.
4. Dhoma e serverave survejohet dhe mbrohet me kamera ne 24 ore, me regjistrim deri ne 1 muaj, me riperseritje.
5. Ambjenti ku ruhen te githa pajisjet e sistemit tone, jane te pajisura me ajer te kondicionuar, me UPS, detektore dhe me fikesa zjarri.
6. Te githa pajisjet ne dhomat e serverave jane te siguruara kunder demtimeve, termeteve apo cdo lloj tjeter rreziku natyror.
7. Kompjuterat personale (PC) ne zyrat e NETSYSCOM Sh.p.k, jane te vendosur ne perputhje me standartet e kerkuara teknike instalimin dhe perdorimin e tyre, ata jane te vendosur ne vende ku personat e paautorizuar nuk kane mundesi te shohin informacionet sensitive qe ndodhen ne to.
8. Instalimi i cfardo programi te nevojshem per kompanin NETSYSCOM Sh.p.k apo transferimi (levizja) behet nga personeli i trajnuar dhe autorizuar nga Menaxheri i kompanise.

   Ne rast se lind nevoja te nxirren jashte ndertesave, duhet te jene po aq te sigurta sa edhe pajisjet qe ndodhen brenda tyre, duke marre parasysh riskun e te

punuarit jashte godinave te kompanise.

9. Te dhenat ne hard-disk per kompjuterat portable, (laptop) enkriptohen duke perdorur programe te miratuara enkriptimi.
10. I gjithe personeli eshte pergjegjes per te garantuar sigurine e aseteve qe jane nen kontrollin e tyre.

Per cdo burim informacioni te kompanise, perdoruesve u jepet akses vetem ne perputhje me funksionet e tyre per kryerjen e detyrave dhe ky akses kontrollohet me rreptesi per te ruajtur integritetin dhe sigurine e aktivitetit.

Hapi i pare i kontrollit te aksesit eshte identifikimi i perdoruesit. Kjo mbulon procedurat per t'u siguruar qe cdo sistem eshte i afte te njohe personat e autorizuar dhe te kryeje veprimet e duhura, ne rastet e perpjekjeve per aksesim te paautorizuar.

4.Menaxhimi i operacioneve

NETSYSCOM ka hartuar nje politike te saj per planifikimin operacional qe ka te beje me operacionet e perditshme te biznesit dhe shperndan detyra njesive te veganta ekzistuese si me poshte:

a) Perfshine marketingun dhe ofrimin e sherbimeve te kompanise sone.
b) Planifikimi i operacioneve percakton planin operues me optimal si dhe planin me te mire operues per sherbim.
c) Pergjegjesit per funksionimin e sistemit jane te ndara sipas personelit

Ne rast te ndryshimit te funksionimit te sistemeve (ndrrim, update apo cdo gje tjeter) ne disponojme backup qe sistemet kryesore mos te dalin jashte sherbimeve.

Personi pergjegjes dokumenton ndryshimin e realizuara nga NETSYSCOM Sh.p.k, krijon nje raport ku pershkruan hapat e ndjekura dhe rezultatet pas ndryshimeve.

Duke u konsultuar me te githa departamentet, personat pergjegjes, zhvillojne dhe mbajne plane per rikrijimin e te gjitha proceseve dhe sherbimeve kritike te aktivitetit, ne rastet e nderprerjeve serioze. Nderprerje te tilla mund te shkaktohen nga shkaqe natyrore, nga aksidente, nga difekte te pajisjeve, nga veprime te qellimshme ose nga difekte te sherbimeve.

5.Menaxhimi i incidenteve

NETSYSCOM Sh.p.k, nepermjet trajnime te njepasnjeshme te personelit, ka bere te mundur qe ne rast incidentesh, personeli pergjegjes eshte ne gadishmeri dhe i mire pergatitur te perballoj cdo incident te mundshem.

Per cdo lloj incidenti, mbahet nje inventor ne pikat e meposhtme dhe nje register risku:

- Shkaku i lindjes se incidentit.
- Menyra e pershkallzimit dhe zgidhjes.
- Koha e shpenzuar per zgidhjen e incidentit.

Pas cdo incidenti, personeli eshte i afte te nxjerr konkluzionin dhe te shmang incidente te te njejtes natyre, si dhe te parapergaditet per nje incidente te tjera.

Sipas llojit te incidenteve, mbahet nje pershkrim i detajuar per tipin, menaxhimin dhe raportimin e incidentit tek eproret perkates.
Ekziston nje sistem menaxhimi per kontrollin e defekteve/incidenteve me ane te te cilit zbulohet cdo problem nga me i vogli tek me i madhi ne kohe reale dhe pas zbulimit te incidentit njoftohen personat e caktuar per marrjen e masave te menjehershme per zgjidhjen emergente te tyre.

Rishikimi i sistemeve mbrojtese dhe procesi i zbulimit te incidenteve rishikohet cdo here sipas ndryshimeve dhe incidenteve te fundit.

Shkeljet ne sigurine e rrjetit me pasoja incidente mesatare ose te renda, trajtohen menjehere dhe i njoftohen Perg'eg'esit te rrjetit, Menaxherit dhe Administratorit te NETSYSCOM Sh.p.k, te cilet marrin masat e nevojshme per te rregulluar incidentin, si dhe merren masa qe te mos perseritet si incident.

Raportimi i incidenteve:

- ✓ Incidentet i komunikohen personit pergeges per registrimin e tyre.
- ✓ Zbatohen procedurat operacionale kur ky incident ndodh duke perfshire ekzaminimin, izolimin dhe masat e rikuperimit.
- ✓ Raportohen te githe procedurat e marra gate procesit te ekzaminimit, izolimit dhe rikuperimit te sherbimin apo sistemit.
- ✓ Raportohen rezultatet e zgidhjes se incidentit dhe vlerat e mbylljes se tij.
- ✓ Merren masa ndaj shkakut te ndodhjes se ketij incidenti perfshire burimet, proceset e punes apo individet.
- ✓ Identifikuesit e incidentit nese nuk jane personi pergeges i menaxhimit te
- ✓ incidenteve nuk nderhyjne ne riparimin e tij por vetem te raportojne tek personi pergjegjes.

Me poshte listojme kategorite e incidenteve:

- 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

Masat per eleminimin e incidenteve

- ✓ Kontrollohen loget e ruajtura nga pajisjet e sistemit.
- ✓ Verifkohet shkaku i incidentit.
- ✓ Analizohet sulmi i pesuar dhe portat e sulmuara.
- ✓ Behet mbyllja dhe izolimi i portave te sulmuara.
- ✓ Rikthehet backupi me te githa konfigurimet bazike.
- ✓ Rishikohen konfigurimet nese jane njelloj me te meparshmet.
- ✓ Ringrejme firewalin e Mikrotiikut pas konfigurimeve.
- ✓ Konsultohemi me stafin ose specialiste te fushes per llojin e incidentit.

- ✓ Trajnohet stafi me qellim mosperseritjen e incidentit.

Ne cdo rast incidenti, ai regjistrohet ne Regjistrin e incidenteve dhe arkivohet sipas ketij regjistri. Regjistri i incidenteve jepet bashke me kete material sigurie, ne fund te tij.

Formulari i raportimit te incidentit:

FORMULARI PER RAPORTIMIN E NJE INCIDENTl TE SIGURISE DHE/OSE CENIMIT TE INTEGRITET1T	
Inforniacion Kontakti	***Emri i Sipermarresit:***
	Emri dhe Mbiemri i personit te ngarkuar me eleminimin e incidenteve te siguri.se dhe/ose cenimit te integritetit:
	Posicioni i Punes:
	Adresa:
	Telefon. e-mail:
Pcrshkrimi i Incidentit te Sigurise dhe/ose Cenimit te Integritetit	***Lloji:***
	Percaktimi se cila rrjete. sisteme ose sherhime preken nu incidenti i s igarise
	Koha e ndodhjes dhe kohezgjatja:
Menaxhimi i incidentit te siguri.se dhe/ose cenimit te integritetit	***Veprimet e ndermarrat te planifikuara per tu ndermarre> per te eleminuar incidenlin e sigurise dhe per te reduktuar pasojat e tij:***
	Masat pas incidentit
Informacione te Tjera te Rendcsishme	***Mesimet e nxjerra***
Data	

6.Menaxhimi i Vazhdimit te Biznesit

NETSYSCOM Sh.p.k aplikon konsultimi me te gjithe sektoret e kompanise, dhe kjo ben te mundur zhvillimin dhe mbajtjen e planeve per rikrijimin e te gjitha proceseve dhe sherbimeve kritike te aktivitetit, ne rastet e nderprerjeve serioze. Nderprerje te shkaktuara nga shkaqe natyrore, nga aksidente, nga difekte te pajisjeve, nga veprime te qellimshme ose nga difekte te sherbimeve.

NETSYSCOM per vazhdueshmerine e aktivitetit perfshijne masat per reduktimin e riskut, per kufizimin e pasojave te shkaktuara prej nje kercenimi qe mund te ndodhe,

dhe per garantimin e rifillimit sa me te shpejte te operacioneve kritike. NETSYSCOM e vazhdueshmerise mundesojne funksionimin ne vazhdimesi te aktiviteteve ne raste demtimesh, difektesh ose humbjesh te sherbimeve apo te pajisjeve.

Ato perfshijne:

a) Identifikimin dhe vendosjen e prioriteteve per proceset kritike te biznesit.
b) Identifikimin e kercenimeve te mundshme qe mund te kene efekt ne keto procese.
c) Percaktimin e ndikimit te mundshem te katastrofave te ndryshme ne aktivitetet e biznesit
d) Identifikimin dhe realizimin e marreveshjeve per gdo pergjegjesi, ne rast gjendje te jashtezakonshme;
e) Dokumentacionin per procedurat dhe proceset per te cilat eshte rene dakord.
f) Edukimin e personelit ne ekzekutimin e procedurave
g) Testimin e planeve.
h) Permiresimin e vazhdueshem te planeve.

Procesi i planifikimit te vazhdueshmerise se aktivitetit siguron, mbajtjen ne pune te proceseve dhe sherbimeve kritike te kompanise. Cdo menaxher eshte pergjeges per NETSYSCOM e vazhdueshmerise se aktivitetit per sistemet dhe pajisjet qe kane ne pronesi te tyre.
Te pakten nje kopje e gdo plani te tille ruhet ne nje vend te sigurt, jashte nderteses, per te siguruar disponueshmerine e tij ne çdo kohe.
Ne rast katastrofash, eshte e domosdoshme krijimi i planeve per ruajtjen e te dhenave, apo sherbimin e ofruar nga kompania jone, dhe rifillimi kohe sa me te shkurter.
Per cdo sistem dhe sherbim krijohet nje plan rindertimi (recovery), i cili mbahet nga nje person i caktuar.

7.Monitorimi, Auditimi dhe Testimi

NETSYSCOM Sh.p.k ka nje sere programesh per monitorimin e rrjetit, logeve dhe sistemeve kritike, ato ruhen me sisteme backup. Te gjitha programet jane ne funksion te proceseve te punes dhe personeli eshte i pergatitur per ti bere balle te gjitha problemeve si ato te parashikuara, si ato te paparashikuara.
Cdo problem qe mund te ndodhe gjate dhenies se sherbimit internet, rregjistrohet dhe dokumentohet qe ne te ardhmen ne rast te te njejtit problem, zgjidhja te jete e shpejte dhe te ulet risku i perseritjes te te njejtit problem.Rrjeti dhe materialet e reja ne NETSYSCOM Sh.p.k testohen ne zyrat e kompanise perpara se te hidhen ne rrjetin kryesor. Ato testohen me mjetet perkatese, sipas llojit te pajisjes qe

do te perdoret.

Cdo testim i raportohet Pergjegjesit te rrjetit perpara se te instalohet ne rrjetin e NETSYSCOM Sh.p.k.

8. Ruajtja e te dhenave personale.

Te dhenat personale te klienteve, ruhen vetem per kontratat dhe trafikun. Te dhenat per kontratat na sherbejne per marredheniet kontraktuale dhe ruajtjen e marredhenies me klientet. Ketu perfshihen, te dhena si emri, adresa dhe informacione per produktet, sherbimet dhe tarifat e perdorura. Komisioneri i te dhenave personale na ka njoftuar disa here rregulloret e tyre si te ruhen te dhenat personale dhe ne i zbatojme ato rregulla.

Per dhenave te klientit, stafi im nuk ka akses ne te dhenat e ruajtura, por ka vetem njeri teknik pergjegjes. Dhe ai i perdor vetem per faturimet dhe kur kerkohet nga institucione te ngarkuara me ligj.

Te dhenat e klienteve i ruajme dhe te administrojme, per nje periudhe 2 vjecare, sic e kerkon Ligji nr. 9918 date 19.05.2008 per "Komunikimet Elektronike ne Republiken e Shqiperise".
Stafi im zbaton rregullat e brendshme te kompanise qe te mbroje te dhenat e klienteve ne menyren me te mire te mundshme. Cdo e dhene e dale nga stafi, konsiderohet si shkelje ligjore dhe shoqerohet me masa disiplinore.

Administratori i NETSYSCOM Sh.p.k

Dede Bukaqeja