A.E. DISTRIBUTION shpk

Masat teknike dhe organizative per sigurine e rrjetit dhe sherbimeve

Siguria e rrjeteve, sistemeve dhe aplikacioneve mbeshtetese

Rrjeti yne do te jete ndertuar ne pjesen me te madhe ne bazen e Sistemit te Routimit Router OS. Trafiku i internetit do te sigurohet nga kompania provider, nepermjet rrjetit me fiber optike te komanise tone. Nepermjet IP statike te subnenit te tyre. Routeri Kryesor Mikrotik do te lidhe te gjithe rrjetin e brendshem te Network Address Translation brenda rrjetit te Kompanise.

Ne kete router do te jene marre masa dhe ndertuar disa rregulla ne firewall per te bllokuar komunikimet e padeshirueshme nga brenda rrjetit dhe nga jashte rrjetit. Per komunikimin e jashtem te Routerit Kryesor jane krijuar rregulla ne firewall per te limituar aksese te padeshiruara.

Lidhja e klienteve me rrjetin qendror do te behet me Protokollin PPPOE (Point to Point Protocol over Ethernet) qe do te thone se ndertohet nje tunel virtual privat (VPN) direkt nga pajisja fundore e klientit per ne routerin kryesor. Kompjuterat do te jene te pajisur me mbrojtje Antivirus dhe firewall te personalizuar ne baze te perdorimit te Kompjuterave. Serverat dhe pajisjet qe do te jene te ekspozuar direkt ne internet nepermjet IP publike do te kene gjithashtu te modifikuar portat e kontrollit dhe firewall te aktivizuar per bllokimin e trafikut te padeshirueshem dhe dhenien e aksesit vetem ne IP publike te listuara ne rregullat e firewall.

Politikat e aksesit te kontrollit

Pergjegjesi i infrastruktures eshte pergjegjes per sigurine e pajisjeve dhe mbikqyrjen e vazhdueshme te aksesit ne rrjet, pajisje dhe sistemet e brendshme te kompanise. Ai u garanton punonjesve te rinj te strukturave perkatese qe u eshte dhene niveli i duhur i aksesimit ne pajisjet dhe ne sistemet e kompanise perfshi ketu llogarite e perdoruesve per kompjuterat, email, 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 cdo 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 gjithashtu e mbikqyr perdorimin e te drejtes per akses ne sistem.

Te gjithe pjesetareve te rinj u jepen instruksione te plota per procedurat e teknologjise se informacionit dhe ne vecanti per kerkesat ne lidhje me ceshtjet e sigurise.

Keto instruksione perfshijne:

1. Perdorimin e pergjithshem te mjeteve te teknologjise se informimit.
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.
6. Rregullat per fjalekalimet.

Kjo behet para se atyre t'u hapet ndonje llogari perdoruesi ose t'u jepen privilegje per te aksesuar sistemet brendshme. Eshte pergjegjesi e Pergjegjesit te burimeve njerezore 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 per mbylljen e llogarise se perdoruesit dhe per heqjen e te drejtave te aksesimit te sistemit teknik, behen para se pjesetari i stafit te largohet fizikisht nga ambienti i punes.

Personi pergjegjes i caktuar per administrimin e rrjetit, informohet menjehere kur ndonje pjesetar i personelit e le punen ose afati i tij i punesimit mbaron per gdo lloj arsyeje. 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 arsye te ndryshme, mund te vazhdojne punen normalisht edhe per nje periudhe mbasi ata te kene kerkuar largimin.

Njoftimi tek Administratori 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. Email-i Perdorimi i llogarive te postes elektronike te Kompanise duhet te jete i pershtatshem dhe ne perputhje me kete politike.

Perdorimet e papranueshme te postes elektronike perfshijne, por nuk kufizohen vetem ne:

- Hapja e dokumentave bashkengjitjur te padeshiruara te postes elektronike pa skanim paraprak;
- Perdorimi i adresave personale te postes elektronike per qellimet e biznesit te Kompanise;

- Dergimi i mesazheve te postes elektronike te padeshiruara, perfshire dergimin e postes junk ose material tjeter reklamues;
- Perdorimi ose falsifikimi i paautorizuar i informacionit per header te postes elektronike;
- Çdo forme ngacmimi permes postes elektronike, perfshire kerkimin e postes elektronike nga ndonje adrese tjeter e-mail, me qellim te ngacmimit ose te mbledhjes se pergjigjeve;
- Dergimi i mesazheve me poste elektronike brenda ose jashte qe permbajne informacione te pakriptuara, te ndjeshme, te korporatave. Nese ekziston ndonje dyshim, keshillohuni me mbikeqyresit ose personin pergjegjes te sigurise; dhe
- Çdo aktivitet i shoqeruar me phishing ose email te krijuar per te mbledhur informacione personale nen pretekste false.

Interneti dhe Media Sociale

Çdo aktivitet ne internet duke perdorur pajisjen ose rrjetin e kompanise duhet te jete ne perputhje me kete politike, politiken e komunikimit dhe kodin e sjelljes dhe etikes se biznesit.

Aktivitetet e papranueshme sociale ne internet perfshijne, por nuk kufizohen vetem ne:
- Shperndarja, shikimi, shkarkimi, ruajtja ose percjellja e materialeve per te rritur;
- Ngacmimi ose ndonje forme tjeter diskriminimi;
- Shperndarja e informacionit konfidencial, pronesor ose informacion tjeter te ndjeshem te Kompanise;
- Shperndarja e çdo çeshtje te brendshme te Kompanise qe mund te jete e demshme per kompanine ose e dobishme per konkurrencen e Kompanise; dhe
- Perdorimi i logos, markes, ose markave tregtare te Kompanise, ose postimi i videove, klipeve te mediave ose imazheve te sponsorizuara nga Kompania, ose imazhe qe i referohen Kompanise.

Ruajtja dhe sherbimet ne cloud

Ne mbrojtje te çdo informacioni te Kompanise, çdo perdorim ose akses ne cloud ose ne rrjetin personal duhet te jete me lejen paraprake te personave pergjegjes se sigurise se Informacionit.

File Sharing

Ne mbrojtje te çdo informacioni te Kompanise, çdo perdorim ose akses ne Platformat File Sharing duhet te jete me lejen paraprake te personave pergjegjes se sigurise se Informacionit.

Mediat e levizshme

Ne mbrojtje te hapesirave ose transmetimit te Informacionit te Kompanise, perdoruesit duhet te perdorin vetem pajisje te autorizuara nga personat pergjegjes se sigurise se Informacionit. Aksesi remote Aksesi remote ne rrjetin e kompanise do te ofrohet nga Kompania per Perdoruesit e autorizuar. Perdoruesit duhet te perdorin nje lidhje te aprovuar nga TIK kur hyjne ne rrjetin e kompanise me akses remote.

Perdoruesit duhet te marrin masa paraprake te arsyeshme per te mbrojtur qasjen ne informacionin dhe rrjetin e Kompanise gjate aksesit remote.

Politikat e pergjithshme te konfigurimit

- Paisjet hardware, sistemet e operimit, sherbimet dhe aplikacionet duhet te miratohen nga Pergjegjesi i sigurise se informacionit si pjese e fazes se para aplikimit.
- Sherbimet dhe aplikacionet te cilat nuk i sherbejne klienteve aktiv behen inaktive.
- Sherbimet dhe aplikacionet duhet te mbrohen me access-lista.
- Te gjitha update-et e hosteve duhet te behen nepermjet kanaleve te sigurta.
- Evente te cilat kane te bejne me sigurine e paisjeve duhet te regjistrohen dhe me pas te auditohen nga pergjegjesi i sigurise se informacionit ku perfshihen:
- Tentativat e deshtuara per te aksesuar paisjet
- Deshtimet per te kerkuar akses te privilegjuar
- Dhunime te politikave te aksesit

Procedurat e menaxhimit te instalimeve te reja

- Ndryshimet ne konfigurime duhet te ndjekin procedurat e menaxhimit te ndryshimeve.
- Pergjegjesi i sigurise se informacionit duhet te ndjeke hap pas hapi te gjitha procedurat ne menyre qe te aprovoje ose jo te gjitha konfigurimet e reja apo ndryshimet perkatese.

Politikat e sigurimit te router-ave

Cdo router ploteson kerkesat minimale te konfigurimit si me poshte:
- Password qe te kalohet ne priviledged mode ruhet i enkriptuar.
- Ndalohen: - Broadcast-et e pa nevojshme ne rrjet. - Paketat qe vijne ne hyrje te router me adrese IP te pa vlefshme.
- Perdoren string-e standarte te kompanise per SNMP
- Rregulla aksesi drejt paisjeve.
- Router-at jane te perfshire ne sistemin e menaxhimit dhe te monitorimit.
- Cdo router apo switch eshte i pajisur me banner ku shkruhet: “Akses i Pa Autorizuar”.
- Telnet nuk lejohet jashte rrjetit, pervec ne rastet kur nje punonjes eshte i lidhur me vpn me rrjetin tone.

Rrjetet Virtuale Private (VPN)

- Punonjesit tanë do te mund te perdorin VPN per te punuar nga shtepite e tyre ne raste emergjente, kur duhet te behet nje nderhyrje e shpejte ne rrjet apo kur duhet te modifikohen dokumenta te ndryshem.
- VPN do te perdoret nga punonjesit e duke perdorur kredencialet e tyre unike ku perfshihet nje username dhe nje password i forte ne menyre qe do te realizojne lidhjen me sistemin tone. Nuk duhet ne asnje rrethane keto te dhena te ndahen apo te perdoren nga te tjere pasi te gjitha masat ndeshkuese do te bien mbi username perkates dhe jo mbi personin i cili ka shkaktuar demet perkatese nga nje nderhyrje e pa deshiruar.
- Punonjesit te cilet mund te perdorin VPN marrin aprovimin me pare nga pergjegjesi i sigurise seinformacionit.
- Te gjithe kompjuterat qe perdoren per te bere lidhjen VPN duhet te jene te update-uar me antiviruset me te fundit.
- Te gjitha te dhenat e VPN dhe gateway konfigurohen nga administrator i rrjetit.

Qeverisja dhe Menaxhimi i Riskut

Ne si kompani e re kemi nje politike te Menaxhimit te Sigurise se Informacionit, e cila percakton kerkesat e Kompanise per mbrojtjen e Aseteve te Informacionit ne perputhje me ligjin ne fuqi dhe politikat, standardet, procedurat dhe udhezimet e Kompanise. 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 politike implementuar duke perdorur nje nderthurje objektivash dhe dokumentim progesesh. Si pjese perpjekjeve te vazhdueshme per permiresimin dhe zbatimin e kesaj politike, ne:

1. Perdorim trajnimin dhe komunikimin me te gjithe punonjesit per tu siguruar qe kjo politike eshte kuptuar dhe vene ne veprim;
2. Vendosim politiken e Menaxhimit te Sigurise se Informacionit ne kulturen dhe praktikat e perditshme, si nje angazhim afatgjate per permiresimin e vazhdueshem te sigurise se informacionit.
3. Sigurojme qe informacioni yne menaxhohet shume mire, duke permbushur tre parimet e sigurise se informacionit: te konfidencialitetit, integritetit dhe disponueshmerise.
4. Sigurojme disponueshmerine e burimeve te nevojshme per te mbajtur nen kontroll Sigurine e Informacionit.
5. Sigurojme qe kontrollet e pershtatshme per sigurine e informacionit jane aktive.
6. Sigurojme qe rreziqet e reja dhe te ndryshueshme, menaxhohen ne menyren e duhur dhe profesionale.

7. Sigurojme qe ne i kuptojme dhe jemi ne perputhje me rregulloret e AKEP dhe kerkesat ligjore qe prekin aktivitetin e punestone.
8. 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.

Masat e mbrojtjes ndaj rreziqeve:

Per te parandaluar instalimin e programeve te rrezikshme punonjesit e kompanise jane te detyruar qe te shkarkojne vetem programe te licencuara. Perdorimi i programeve antivirus nga kompani te licensuara parandalon dhe eviton efektet e ketyre viruseve. Aktualisht, kompania jone do te kete ne perdorim Kaspersky Endpoint Security Cloud. Antivirus menaxhohet nga pergjegjesi i infrastruktures, duke monitoruar sigurine e pajisjeve ne nivel qendror. Firewall eshte mjeti mbrojtes me i rendesishem per mbrojtjen nga sulmet e jashtme. Firewall eshte gjithe kohes aktiv dhe konfigurohet ne baze te kerkesave te komunikimit. Sistemet operative te perdorur Windows dhe windows server jane te licencuar, duke mundesuar perditesimet periodike, per te evituar cdo infiltrim te mundshem te programeve te rrezikshme.

Siguria e Burimeve

Njerzore Cdo punonjes 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 kompanise, 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 vecanta ose per ekzekutimin e proceseve te vecanta.

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 kompanisë tone mbi:

- konfidencialitetin
- sigurine e informacionit
- te dhenave personale.

Siguria e sistemeve dhe Pajisjeve

Siguria Fizike Dhoma e Serverave dhe te gjithe aparaturave qe mundesojne lidhjen e rrjeteve te komunikimit do te jete e vendosur ne nje ndertese, qe ploteson te gjitha kriteret e sigurise se objekteve me rendesi te vecante. Normat e sigurise perfshijne sistemin elektronik te alarmit, survejimin me kamera qe transmetojne imazhe ne kohe reale tek personeli i autorizuar per mbikqyrjen dhe mirembajtjen. Aksesi fizik eshte i rezervuar per nje numer te vogel personash.

Ambjeti do te mbahet ne temperature konstante dhe pastrohet rregullisht per pluhura dhe grimca qe trasportohen nepermjet ajrit, qe mund te demtojne procesoret dhe sistemet e ventilimit te pajisjeve. Rrjeti i ISP do te jete i mbrojtur nga Firewall per te evituar sulmet ne porta te ndryshme te aksesit. Rrjetet e menaxhimit do te jene te vendosura ne VLAN te vecuar dhe aksesohen vetem nga sherbimet VPN.

Kontrolli dhe vezhgimi i aksesit ne rrjet do te monitorohet nepermjet Logfile te serverave. Serverat dhe routerat do te perditesohen me versionet me te fundit te sistemeve operative dhe normave te sigurise nga burime zyrtare te kompanive qe ofrojne suportin e ketyre sistemeve.

Menaxhimi i operacioneve

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

- Perfshine marketingun dhe ofrimin e sherbimeve te kompanise sone.
- Planifikimi i operacioneve percakton planin operues me optimal si dhe planin me te mire operues per sherbim.
- Pergjegjesit per funksionimin e sistemit jane te ndara sipas personelit. Ne rast te ndryshimit te funksionimit te sistemeve (nderrim, update apo cdo gje tjeter) ne disponojme backup qe sistemet kryesore mos te dalin jashte sherbimeve.

Personi pergjegjes dokumenton ndryshimet e realizuara, 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.

Menaxhimi i incidenteve

Kompania jone, nepermjet trajnimeve te njepasnjeshme te personelit, do te beje te mundur

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

Pas cdo incidenti, ekipi i ndjekjes se incidenteve do te jete i afte te nxjerr konkluzionin dhe te shmange incidente te te njejtes natyre, si dhe te parapergaditet per nje incidente te tjera.

Raportimi i incidenteve:

- Incidentet i komunikohen personit pergjegjes 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 pergjegjes 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 shërbimit
- Demtim hardware apo software i pajisjeve
- Vjedhje e pajisjeve
- Hack-im
- Infektim nga viruse te ndryshme
- 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.

Menaxhimi i Vazhdimit te Biznesit

Kompania jone do te aplikoje konsultimin 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. Kompania jone per vazhdueshmerine e aktivitetit perfshin 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.

Ato perfshijne:

- Identifikimin dhe vendosjen e prioriteteve per proceset kritike te biznesit.
- Identifikimin e kercenimeve te mundshme qe mund te kene efekt ne keto procese.
- Percaktimin e ndikimit te mundshem te katastrofave te ndryshme ne aktivitetet e biznesit.
- Identifikimin dhe realizimin e marreveshjeve per cdo pergjegjesi, ne rast gendjeje te jashtezakonshme;
- Dokumentacionin per procedurat dhe proceset per te cilat eshte rene dakord;
- Edukimin e personelit ne ekzekutimin e procedurave
- Testimin e planeve.
- Permiresimin e vazhdueshem te planeve.

Plani i vazhdimesise se biznesit hyn ne veprim kur nje incident ndikon ne operacionet e biznesit.

Monitorimi, Auditimi dhe Testimi

Kompania disponon nje sere programesh per monitorimin e rrjetit, logeve dhe sistemeve kritike, ato do te ruhen me sisteme backup. Te gjitha programet jdo te jene 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, 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 pajisjet e tjera kompjuterike 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 Administratorit te rrjetit perpara se te instalohet ne rrjetin tone
Ruajtja e te dhenave personale

Te dhenat personale te klienteve, do te 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. Per dhenave te klientit, stafi im nuk do te kete akses ne te dhenat e ruajtura, por do te kete vetem njeri teknik pergjegjes. Dhe ai vetem per faturimet dhe kur kerkohet nga institucione te ngarkuara me ligj.

Te dhënat e logeve te klienteve do ti ruajme dhe te administrojme, per nje periudhe 2 vjecare, sic e kerkon Ligji nr. 54/2024 per "Komunikimet Elektronike ne Republiken e Shqiperise".

Stafi im do te zbatoje 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.