



Soft&Solution

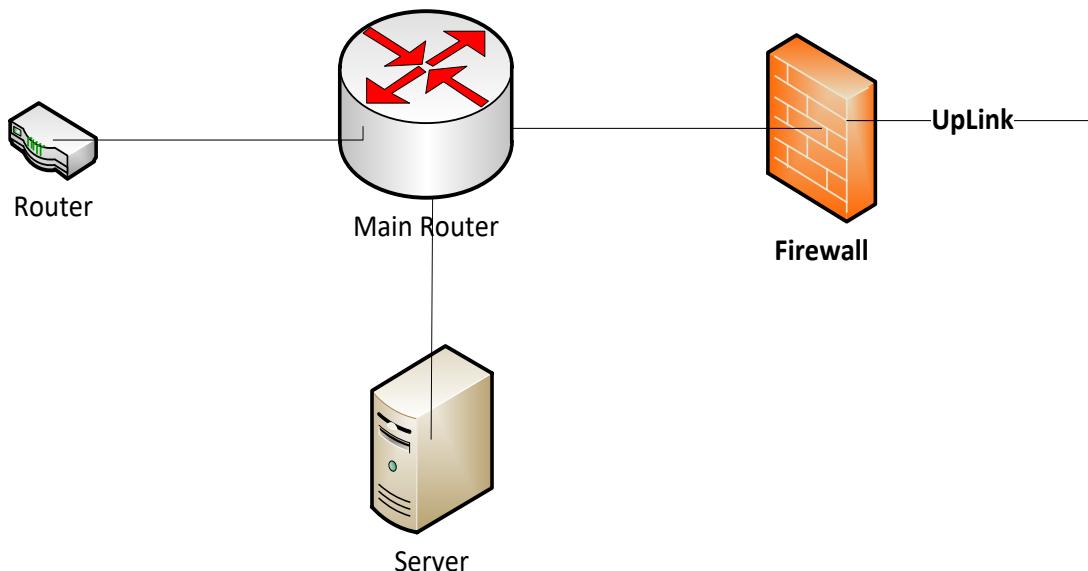
Focus on **Solutions** not just **Code!**

Siguria e Sistemeve dhe Pajisjeve



Soft Solutions ka ndertuar një rrjet te komunikimeve elektronike me fibra optike. Rrjeti nuk eshte i madh dhe per faktin qe nuk ka shume klientë te lidhur. Kemi vetëm klientë preferenciale te cilet marrin shembim me kapacitet te larte.

Skematikisht rrjetin e paraqesim ne skemen me poshte:



Routeri kryesor i cili eshte dhe firewall eshte router 5545-X.

Pajisjet e tjera jane routeri fundore te cilet jane pjesa e rrjetit te klientit.

Aksesi ne internet per klientët realizohet me lidhje direkte nga Routeri qendror dhe ka kufizime ne Bandwith nga routeri bazuar ne IP e caktuar.

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

Disa nga funksionet e pajisjeve ruterave qendrore Cisco jane:

1. Krijim rrjeti te qenderzuar
2. Implementim sigurie i te dhenave
3. Percaktimi i bandwith bazuar ne IP.
4. Segmentim i rrjetit te brendshem aty ku eshte e nevojshme
5. 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 Cisco 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



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

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 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 ndryshme te drejtash ne cdo pajisje si pjese e kompanise.

Përgjegjës per çështjet e sigurisë eshte Znj. Arjola Koromani, Administrator i Sistemit dhe përgjegjës per sigurinë dhe menaxhimin e aseteve përkatës.

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 paautrizuar 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 menjehershems 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 perqigjes. Gjithashtu gjate ketij stimulimi matet edhe riskun gjate periudhes se thyerjes se sistemit dhe kohes se perqigjes.

Sistemet operativ janë Windows 10 te cilet e kane antivirusin te perfshire ne sistem.

Sigurimi i Medisit nga Katastrofat Natyrore

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

Ne cdo ambjent jane vendosur pajisjet e izolimit dhe ndalimit te zjarrit. Cdo sistem 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 bllokuar rreziqet 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 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 elektrike per nje periudhe



ISO: 14001:2004, 18001:2007, 20000-1:2011, 50001:2011, PASS 99:2012, 22301:2012, 27001:2013, 55001:2014, 9001:2015
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 nederprerje te saj.

Politikat e Kontrollit te Aksesit

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 eshte i autorizuar ne menyre specifike.
- Aksesi ne informacion eshte i kontrolluar bazuar ne kerkesat e kompanise, dhe rregullave specifike te percaktuara per cdo sistem informacioni.
- Te gjithe punonjesit e kompanise aksesojne vetem ato asete dhe sisteme te informacionit te cilat jane te nevojshme per te permbushur detyrat e tyre te punes.
- Te gjithe perdoruesit janë pajisur me një deklarate me shkrim ose elektronike mbi te drejtat e aksesit te tyre, termat dhe kushteve per perdorimin e ketyre te drejtave.
- Llogaria e perdoruesit rishikohet çdo 2 muaj per privilegjet e duhura.
- Llogarite e perdoruesve te cilet largohen nga kompania hiqen menjehere pas perfundimit te punes se tyre.
- Te gjitha privilegjet e perdoruesve fillestar dhe ekzistues caktohen nepermjet një autorizimi te Administratorit te kompanise.
- Te gjithe perdoruesit duhet te zbatojne Politiken e Fjalekalimit.
- Politika e Fjalekalimit perben krijimin e një fjalekalmi kompleks ne te cilin perfshihen 4 lloje te ndrryshme kategorish te karaktereve sidhe një gjatesi jo me pak se 8 karaktere.
- Te gjitha fjalekalimet qe i perkasin Administratorit te Sistemit i cili ka dhene doreheqje ose eshte pezulluar 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 cdo rrjet.

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

Mekanizmat e duhur per kontrollin e rrugezimit janë implementuar per te kufizuar rrjedhen e informacionit ne rruget e rrjetit te percaktuar brenda kontrollit te kompanise. Kontrollet e rrugezimit te rrjetit bazohen 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 kane një arkitekturë te mbyllur dhe shume te sigurte.

Monitorimi

Te gjitha detajet e ngjarjeve lidhur me sistemin e informacionit ruhen per 1 muaj per sistemet e zakonshme dhe 2 muaj per sistemet kritike. Pas kësaj periudhe këto informacione arkivohen dhe ruhen ne arkive per 2 vjet.



ISO: 14001:2004, 18001:2007, 20000-1:2011, 50001:2011, PASS 99:2012, 22301:2012, 27001:2013, 55001:2014, 9001:2015

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

Politika e Integritetit te Sistemeve dhe Rrjetit

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

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

Te gjithe punonjesit qe perdorin pajisjet e kompanise 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 opzionin scan paraprakisht.
- Te tregojne kujdes kur kopojne materiale.
- Te tregojne kujdes kur hapin materiale nga mjete te tilla si USB ose CD. Duhet te shtypin opzionin scan paraprakisht.
- Te skanojne te gjitha mjetet e jashtme per viruse perpara se ti perdorin.
- Te njoftojne me email Personin perqejges 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 standartet e percaktuar ne kete politike.
- Perditesohen sa here eshte e mundur ne baze te sistemit te antiviruseve cdo produkt qe kryen funksionin e nje antivirusi.
- Personi perqejges per sistemet e antiviruseve mbedh log-et nga keto sisteme per te analizuar, identifikuar edhe eleminuar mundesi te tjera te mundshme te sulmeve nga antiviruset.

Veprimet e Rikuperimit

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

Niveli i Prioritetit	shkrimi i Sistemit apo sherbimit	Koha e Pergjigjes
Kritike	<ul style="list-style-type: none"> -Sistemi apo Sherbimi eshte jo aktive -Pjese kritike te Sistemit apo Sherbimit nuk eshte funksional -Veprintari jashte standartit te Sistemit apo Sherbimit -Humbje e te Dhenave sensitive te kompanise 	0-6 Ore
I Larte	<ul style="list-style-type: none"> -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

Siguria dhe mbrojtja e te dhenave personale

Soft Solution e konsideron sigurine e te dhenave personale nje detyrim ligjor shume te rendesishem si dhe nje detyrim vetjak per te permbushur sigurine e te dhenave personale te abonenteve por edhe te kompanise dhe informacionit ne ruajtje, procesim dhe transmetim dhe gjithe hallkat e sistemit. Te dhenat personale ne kompanine time, te jane te aksesueshme vetem nga personeli i autorizuar per qellime ligjore te autorizuara. Autorizimi leshohet vetem nga uen si administrator i shoqerise. Gjithashtu, te dhenat personale ruhen ne nje kompjuter te vecante pa lidhje me rrjetin dhe pa akses ne internet. Kompjuteri sigurohet me username dhe password.

Nje pjese e rendesishe e te dhenave personale, sigurohen nga kontratat me abonetet dhe keto sherbjne vetem per qellimet e biznesit dhe marketingut, por ne asnjë moment nuk i transmetohen ndonje provideri tjeter apo individi tjeter. Perjashtim do te behet vetem nese do te kerkohen nga institucionet Shqiptare te ngarkuara me ligj ndaj te cilave kemi detyrimin ligjor nga KMDPDI per tua vene ne dispozicion. Ndersa fizikisht kontratat ruhen ne kasaforte me celes.

Ne kete menyre mbrojme te dhenat personale te ruajtura ose te transmetuara nga aksidentet apo nga shkatterimi i kunderligjshem, humbja ose ndryshimi aksidental dhe ruajtja, perpunimi, aksesi apo zbulimi i paautorizuar ose i jashteligjshem. Vetem nje person me autorizim nga Administratori ka te drejte te perdore keto te dhena vetem per qellime faturimi.

Ne sigurojme implementimin e politikave te sigurise nga cdo punonjes imi, lidhur me perpunimin e te dhenave personale.