REPUBLIKA E SHQIPERISE

Subjekti juridik "KLOBES" shpk Nipti - L06530801O

Lënda: *Raporti mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve*

Korrik 2018

I. Manaxhimi i riskut

1.1. Politika e përgjithshme e sigurisë së informacionit

Më poshtë përshkruhet politika e përgjithshme, e cila ofron rregulla dhe udhezime për përdoruesit e informacionit brenda kompanisë. Përmes kësaj politike përdoruesit duhet të:

- ❖ Përdorin sistemet kompjuterike vetëm për qëllime të biznesit
- ❖ Ruajnë privatësinë dhe konfidencialitetin e të gjitha të dhënave konfidenciale dhe institucionale.
- ❖ Përdorin User ID unike dhe fjalëkalime personale sekrete për të hyrë në sistemet kompjuterike.
- ❖ Përdoruesit janë përgjegjës për të gjitha aktivitetet që ndodhin me User-ID e tyre.
- ❖ Identifikohen nga të gjithë sistemet, kur lënë një sistem kompjuterik pa mbikëqyrje.
- ❖ Raportojne menjëherë shkeljet e sigurisë.
- ❖ T'i përmbahen procedurave të kontrollit për viruse. Të gjithë software-ve të instaluar ose të shkarkuar nga burime të jashtme përmes internetit duhet të skanohen me software për zbulimin e viruseve para se të perdoren.
- ❖ Punojnë në përputhje me të gjitha licencat software-et e palëve të treta. Çdo software pa leje duhet të hiqet menjëherë nga kompjuterat e kompanisë.

Të gjithë përdoruesit duhet të ndjekin parimet e kompanisë në lidhje me përdorimin e burimeve dhe të ushtrojë gjykim të mirë në përdorimin e internetit.

Përdorimi për kryerjen e funksioneve të punës përfshin:

- ❖ Komunikimi midis punonjësve dhe jo-punonjësve për qëllime të biznesit.
- ❖ IT teknike mbështetje shkarkimit përmirësimit të programeve.
- ❖ Shqyrtimi i vendeve të mundshme shitësi ëeb për informacionin e produktit.
- ❖ Referenca rregullator ose informacione teknik
- ❖ Detyra kerkimore

Çdo kompjuter i lidhur në internet ka një adresë unike, e njohur si një adresë IP. Ajo merr

formën e katër grupeve të numrave të ndarë nga pika, për shembull: 10.5.50.89 Është ky numër që në fakt ju lejon të dërgoni dhe të merrni informacion në internet. Në varësi me llojin tuaj të shërbimit, IP adresa juaj mund të jetë:

- Dinamike, që do të thotë se ndryshon në mënyrë periodike
- Statike që është caktuar në mënyrë të përhershme për ju për aq kohë sa ju te keni shërbimin tuaj.

- IP e bredshme , qe do te thote qe te jep mundesine e lundrimit ne internet te maskuar (NAT) nepermjet nje ip reale. Dhe eshte me I mbrojtur nga

- IP REALE eshte ip qe

Adresa e juaj IP në vetvete nuk ofron informacion personalisht të identifikueshme. Për të evituar problemet që vijnë nga perdorimi i IP-ve publike rekomandohet ndryshimi i portave të shërbimeve bazë si SSH ose HTTP, si dhe përdorimi i fjalkalimeve që përmbajnë shkronja, numra dhe shenja të vecanta.

Kur ju vizitoni një faqe interneti në përgjithsi përdoret protokolli HTTP i cili nuk ofron norma të mjaftueshme sigurie për të mbrojtur informacionet të cilat përcohen nëpërmjet këtij protokolli.
Ky protokoll përdoret për përcimin e informacioneve me ndjeshmeri të ulët për përdoruesit. Nëse ju tansmetoni informacione personale me ndjeshmeri të lartë ju lutem sigurojuni që faqja juaj e internetit supporton protokollin HTTPS, që përdor metodën e enkriptimit për përcimin e informacioneve. Për të garantuar moskompromentimin dhe integritetin e informacioneve, ne ju rekomandojmë përdorimin e shërbimit VPN i cili izolon lidhjen tuaj nga burimi në destinacion me një tunel virtual i cili përcon vetëm informacione të enkriptuara dhe përmban të gjitha mjetet e duhura për të evituar kompromentimin e informacioneve.

1.2. Politika e sigurisë dhe mbrojtjes së të dhënave personale

Lidhja mes abonentit fundor dhe qendrave të shpërndarjes bëhet nëpërmjet protokollit PPPoE. Ky protokoll lejon krijimin e nje tuneli virtual mes pajisjes ku konfigurohet për protokoll dhe routerit kryesor. Lidhja mundësohet nëpërmjet protokollit RADIUS dhe software Radius manager i instaluar mbi linux sic do të përshkruhet edhe më poshtë në këtë raport. Ky model shërbimi mundëson privatësi të plotë të klientit dhe eviton situatat me “man in the middle”, ose

packet sniffing që kompromentojnë integritetin e të dhënave që kalojnë në rrjet. Paketat dixhitale që bëjnë të mundur transmetimin e informacionit enkriptohen me PAP ose CHAP që sigurojnë integritetin e informacionit deri në destinacion, e ndërtuar në modelin e transportit pikë me pikë ku nyjet fizike shërbejnë vetëm si ura që bëjnë lidhjen fizike në shtresën e 2-të të modelit OSI . Destinacioni është Routeri që ndodhet në ambjentet e kompanisë. Nga ky router i jepet rrugë trafikut që del nga rrjeti i kompanisë tonë për në internet (kerkesa per te bere lidhjen, "3 way handshake" dhe ngarkimi i informacioneve ose degimi i mesazheve nepermjet internet protokoll), dhe pjesa me e madhe e trafikut që behen nga jashte rrjetit për tek aplikacionet që kanë kërkuar të dhena nga server të ndryshme. Ky router është i perditsuar me vesionet e fundit te Router OS dhe i mbrojtur me firewall. Aksesi në router është i limituar vetem për personelin e autorizuar nga Klobes shpk. Në rast të njoftimit për probleme teknike ose kompromentim të të dhënave nga klienti fundor bëhen verifikimet e detajuaja te Logfile si në routerin kryesor të kompanisë si në roterat fundore. Bëhen provat e nevojshme dhe në fund bëhet përditsim i software të pajisjeve dhe të dhënat e llogarive në router ndryshohen.

1.3. Manaxhimi i riskut

Shkelja e sigurisë së informacioni mund të ketë pasoja serioze në kompani. Disa shembuj të llojeve të kërcënimeve të siguresë së informacionit në kompani përfshijnë:

- Infektimi nga viruset e ndryshme

  Viruse kompjuteri: Një virus kompjuterik është një pjesë e vogël e softëare që mund të përhapet nga një kompjuter të infektuar në tjetrin. Viruset mund të korruptojnë , të vjedhin, ose në fshirjen e të dhënave në kompjuterin-tuaj deri ne fshirjen e çdo gjëje në hard drivin tuaj. Një virus mund të përdorë gjithashtu edhe programe të tjera si programin tuaj e-mail për të përhapur veten në kompjuterë të tjerë. **Trojan Horse:** Janë programe kompjuterike që vinë futen në kompjuterin tuaj në momentet kur ju instaloni programe të njohura duke menduar që janë të sigurtë. Kto programe sapo instalohen në kompjuterin tuaj fillojnë të grumbullojnë informacione që mund të jenë fjalkalime ose të dhëna personale. **Worms**: Një worm është një program kompjuterik që mund të kopjojë veten nga një kompjuter në tjetrin, pa nevoj të ndërveprimit njerëzor. worms mund të përsëritet në vëllim të madh dhe me shpejtësi të madhe. Për shembull, një krimb mund të dërgoni kopje të vetë për çdo kontakt në librin tuaj adresën email dhe pastaj

dërgojnë veten në të gjitha kontaktet në librat e kontakteve tuaj 'adresave. **Botnet**: Një botnet është një grup i kompjuterëve të lidhur në internet që janë kompromet uar nga një haker duke përdorur një virus kompjuteri apo kalë trojan. Një kompjuter individual në grup është i njohur si një "mumje" kompjuter. **Spam**: Spam në kontekstin e sigurisë është përdorur kryesisht për të përshkruar email spam-mesazhe te padeshirueshme në kutinë tuaj të postës elektronike. Qëllimi i spam është reklamimi i një produkti ose shërbimi që do të cojë në instalimin e programeve të padeshiruara për kompjuterin tuaj dhe aksesimi i të dhënave të ndjeshme që kanë të bëjnë me transferat bankare ose pagesat e ndryshme nëpërmjet internetit. **Phishing**: Është nje mënyrë shumë e përhapur për marrjen e inforamcioneve te ndryshme nëpërmjet dublikimit të adresave dhe shërbimeve të njohura në internet. Praktikisht njerëz me qëllime për të marrë informacione të rezervuara për faqe të ndryshme si rrjetet sociale, llogarite e E-mail, llogaritë bankare me të cilat kryhen transaksione, ndërtojne faqe nga pikpamja vizive të ngjashme për të dhënë iluzionin sikur jeni duke përdorur faqet zyrtare të shërbimeve që kërkoni të përdorni.

SSH atack: janë skripte të automatizuara që sulmojnë portat e paracaktuara të serverave që janë të ekspozuar direkt në Internet. Këto skripte përdorin mijëra passëorde të ndryshme në periudha të shkurtra kohore për të aksesuar serverin tuaj.

- Keqperdorimi i informacionit nga stafi
- Dështimet e sistemit
- Aksesi i paautorizuar nga të huajt, duke përfshirë konkurentet apo hakerat
- Punonjesit e pakenaqur
- Mashtrimi ose vjedhja

Në kompaninë tonë siguria e informacionit shihet si dicka që mund minimizoje dhe të parandalojë cështje që ndikojne në reputacionin dhe në besimin klientëve dhe furnitorëve tonë.

1.4.Masat e mbrojtjes ndaj rreziqeve

Për të parandaluar instalimin e programeve të rrezikshme punonjësit duhet të sigurohen që po shkarkojnë programet e kerkuara në faqet zyrtare të kompanive që ofrojnë shërbimet e kërkuara. Përdorimi i programeve antivirus nga kompani të licensuara parandalon dhe eviton efektet e këtyre viruseve. Duhet të bëhet kujdes të disponohen versione të përditsuara periodikisht të pragrameve mbrojtëse antivirus.

Firewall është mjeti mbrojtës më i rëndësishëm për mbrojtjen nga sulmet e jashtme. Rekomandohet personalizimi i firewall në bazë të kërkesave të komunikimit dhe mbajtja e tij aktive në të gjitha rastet.

Te përdoren sisteme operative të licensuar, te cilat perditsohen periodikisht me masat e nevojshme te sigurisë, për të evituar çdo infiltrim të mundshëm të programeve të rrezikshme për integritetin e sistemeve tuaja.

Për shërbimet dhe transaksionet bankare rekomandohet perdorimi i fjalkalimeve të komplikuara që përmbajne shkronja numra dhe shenja te vecanta. Përpara se të përdoren sherbimet duhet të verifikohet URL ne browers dhe te verifikohen te dhenat e certifikates digitale per ndonje anomali te mundshme .

Aktivitete të tjera të veçanta që janë të ndaluara rreptësisht përfshijnë:

• Përdorimi i informacionit konfidencial që nuk është brenda fushëveprimit të punës së dikujt.

• Keqpërdorimi. (perdorimi pa autorizim përkatës, duke ndryshuar kompaninë ose duke ndryshuar informacionin e personelit.

• Çdo veprim te paautorizuar që qellimisht dëmton ose prish sistemet apo rrjetet informatike, u ndryshon punën e tyre normale, ose i bën ata të mosfunksionojne pa marrë parasysh vendndodhjen ose kohëzgjatje.

• Futja me paramendim ose nga pakujdesia e viruseve kompjuterike, Trojan horses ose programe të tjera të dëmshme në sistemet e kompanisë apo rrjeteve ose në sistemet dhe rrjetet e jashtme.

• Dekodimi i paautorizuar apo përpjekje për dekodim te çdo sistemi apo fjalëkalimi te përdoruesit.

• Përdorimi, transmetimi, dyfishimi ose marrja vullnetare e materialit që shkel të drejtat e autorit, markë tregtare, sekretet tregtare ose të drejtave të patentës të ndonjë personi ose organizate.

• Shkarkim te paautorizuar te ndonjë programi shareëare për përdorim, pa autorizim paraprak nga Departamenti i IT-së dhe menaxherit të përdoruesit.

• Çdo sjellje që do të përbëjnë ose nxisin një vepër penale, të çojë në përgjegjësi civile, ose shkel ndonjë rregullore, lokale, shtetërore, ligjeve kombëtare dhe ndërkombëtare.

• Blerja, ruajtja, shpërndarja, krijimi, postimi, transmetimi ose marrja vullnetare e çdo

informacioni të paligjshem, fyes, shpifës, kërcënues, materiale ngacmimi duke përfshirë por jo kufizuar në komentet në bazë të racës, origjinës kombëtare, gjinisë, orientimit seksual, moshës, aftësisë së kufizuar , feja, apo bindjet politike.

II. Siguria e burimeve njerzore

2.1.Kontrollet e background-it

Stafi është i kualifikuar nga ana profesionale dhe plotëson kriteret e sigurisë për të mbështetur cdo etapë të procesit dhe mirëfunksionimit të sistemeve.

Personeli merr pjesë në trajnime dhe konferenca të perbashketa me partner biznesi të kompanisë tonë për të ndarë eksperiencat dhe për tu informuar mbi ndryshimet e fundit në fushën e telekomunikacionit

III. Siguria e sistemeve dhe Pajisjeve.

3.1.Siguria Fizike

Dhoma e Serverave dhe te gjithe aparaturave qe mundesojne lidhjen e rrjeteve te komunikimit eshte e vendosur ne nje ndertesë, qe ploteson te gjitha kriteret e sigurise e 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 mbahet ne temerature 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 eshte i mbrojtur nga Firewall per te evituar sulmet ne porta te ndryshme te aksesit. Server i VoIP eshte i mbrojtur nga sherbimi Fail2. Rrjetet e manaxhimit jane te vendosura ne VLAN te vecuar dhe aksesohen vetem nga sherbimet VPN. Kontrolli dhe vezhgimi i aksesit ne rrjet monitorohet nepermjet Logfile te serverave.

Serverat dhe routerat përditsohen me versionet më të fundit të sistemeve operative dhe normave të

sigurisë nga burime zyrtare të kompanive që ofrojnë supportin e këtyre sistemeve.

3.2.Siguria e rrjeteve, sistemeve dhe aplikacioneve mbështetëse

Përshkrim i strukturës së rrjetit dhe mjeteve mbrojtëse

Rrjeti i KLOBES është ndërtuar në pjesën më të madhe në bazën Sistemit te Routimit Router OS të kompanisë Mikrotik. Praktikisht trafiku i internetit vjen nga kompania partnere Abissnet, nëpermjet rrjetit me RADIO LINK dhe FIBER OPTIKE pranë komanisë tonë. Nepermjet IP statike te subnenit 77.242.21.90/28 ne Routerit e KLOBES dhe është i konfiguruar si Gateway 77.242.21.89 të Abissnet. Ne kete router nuk ka masa mbrojtese me firewall per efekt te lirise se perdorimit te gjithe sherbimeve. Ndarja, Routimit behet ne Routerin kryesor te KLOBES i cili gjendet ne ambjentet e ku dorezohet sherbimi nga Abissnet. Nga routeri kryesor ka active nje dalje me kabull rrjeti RJ45 dhe nje dalje SFP fiber. Njera dalje shkon ne shperndares rrjeti (Swith) ku jane te lidhur Radio Access Point te konfiguruara si ura kalimi (BRIDGE) qe sherbejne per te lidhur pajisjet radio fundore te klientit. Dalja e dyte me SFP nga Routeri Kryesor shkon ne OLT qe perdoret vetem per aksesimin nga klient e lidhur me FIBER OPTIKE ,

Routeri Kryesor Mikrotik qe lidhin te gjithe rrjetin e brendshem te Network Address Translation brenda rrjetit te Kompanise. Ne kete router jane marre masa dhe jane ndertuar disa rregulla ne firewall per te bllokuar komunikimet e padeshirueshme nga Brenda rrjetit dhe nga jashte rrjetit.

- Per komunikimin e brendshem te rrejtit eshte ndertuar SISTEMI HOTSPOT nga Mikrotik qe devijon apo dergon te gjitha tentativat e mbrenshme te te gjitha IP apo portat.
- Per komunikimin e jashtem te Routerit Kryesor jane FIREWALL te ndryshme per te shmangur aksese te padeshiruara

Lidhja e klienteve me rrjetin qendror 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.

Ky system suportohet direkt nga Protokolli RADIUS dhe per te implementuar kete protokoll perdoret Software nga DMA Softlab, “Radius Manager”. Kompjuterat e personelit dhe serverat e faturimit jane te lidhur ne rrjetin e NAT te lidhur pas router Mikrotik me IP te lidhjes WAN 1.1.1.5. Si rrjedhoje keto kompjutera jane te mbrojtur nga sulmet direkte nga Firewall I router Mikrotik. Kompjuterat jane te pajisur me mbrojtje Antivirus dhe firewall te personalizuar ne baze te perdorimit te Kompjuterave. Serverat dhe pajisjet qe jane te ekspozuar direkt ne internet nepermjet IP publike kane 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.

Ketij Materiali i eshte bashkangjitur dhe nje Topologji e rrjetit ne formation “.png” qe pasqyron lidhjet logjike te rrejtit te ndertuar ne kompanine KLOBES

3.3.Politikat e aksesit te kontrollit

Kontrolluesi i të dhënave ka për detyrë për të kufizuar aksesin në të dhënat personale në bazë ", duhet të dini". kufizime më të mëdha të aksesit apo kontrollit duhet të zbatohen për të dhënat më të ndjeshme. Kontrolluesi i të dhënave duhet të jetë i vetëdijshëm për përdoruesit e ndryshëm që përdorin sistemet e tyre / të dhënat dhe kërkesat e tyre. Llojet e ndryshme të përdoruesve mund të përfshijnë:

Inxhinieret e rrjetit

Stafi i teknikeve;

Partnerët e biznesi
Klientët

Kërkesat e ndryshme të secilit prej këtyre llojeve të përdoruesit dhe privilegjet e tyre për akses në të dhënat personale garantohet vetem ne rastet te dakortesise se te dyja paleve te perfshira, si pala qe kerkon akses te te dhenave si pala qe mbart dhe zoteron te dhenat mbi vetven, personin qe perfason ligjerisht ose biznesin. Natyra e aksesit të lejuar per një përdorues te teknologjise se mundesuar nga KLOBES duhet të vendosen dhe rishikohen në baza të rregullta. Informacionet me ndjeshmeri te Larte transportohen te enkriptuar me RSA nga burimi deri ne destinacion nepermjet Protokolleve qe i supportojne keto masa sigurie. Nga personeli jone nuk eshte e mundur aksesimi i ktyre te dhenave ne asnje rast. Ne cdo situate qe krijon mosbesim

behet nje shqyrtimi i detajuar i sistemeve nga nje grup punonjësish te kompani ë ose ju drejtohet kompanive te specializuara per analizimin e te dhenave te hyrje daljeve dhe detektimit te problemeve ne sistem. Kontrolluesit e të dhënave duhet të ketë procedura në vend për të menaxhuar qarkullimin e stafit, duke përfshirë tërheqjen e pajisjeve magazinimit të të dhënave dhe heqjen e shpejtë të lejeve të qasjes.

Pa marrë parasysh atë kontrollet teknike apo fizike qe janë të vendosur në një sistem, masa më e rëndësishme e sigurisë është të sigurojë që personeli janë të vetëdijshëm për përgjegjësitë e tyre.

Fjalëkalimet nuk duhet të shkruhen dhe të majtë në vende të përshtatshme.

Fjalëkalimet nuk duhet të ndahet në mesin e kolegëve

Bahkangjitjet e-mail te papritura nuk duhet të hapen nëse me pare nuk kontrollohen nga nje program antivirus

Trajnimi efektiv të punonjësve në lidhje me rreziqet e kompromisit të të dhënave, roli i tyre në parandalimin dhe si të reagojnë në rast të problemeve mund të jetë një linjë shumë të efektshme e mbrojtjes.

IV. Menaxhimi i Operacioneve

4.1.Procedura operacionale

Personeli ka te percaktuara rregulla strikte në performimin e cdo veprimi, të cilët janë të ndarë sipas pozicionit, që ato kane në kompani

Cdo procedurë operacionale raportohet dhe dokumentohet prane zyrave tona ne fund te cdo dite pune.

Cdo operacion që përfshin më shumë se 10% të infrastruktures paraprihet me përgatitje për minimizimin e kohës në të cilën ndërpritet shërbimi.

4.2.Menaxhimi i burimeve

Për rrjete tona të televizionit dhe internetit është shumë i rendesishëm furnizimi i vazhdueshem me energji elektrike. Aparaturat tona janë të mbeshtetura nga dy sisteme backup power me invertera te posatshem.

Burime te tjera perfshijne lidhjen e internetit nga ISP jone. Kjo linje nuk eshte e dubluar per momentin. Nepermjet kesaj lidhje interneti behet edhe transmetimi i zerit nepermjet IP me protokollin SIP.

V. Menaxhimi i incidenteve

5.1.Procedura e menaxhimit të incidenteve

Ky plan përshkruan hapat që duhen ndjekur në rast se të dhënat e sigurisë kompromentohen.

Ekipi i reagimit ndaj incidenteve krijohet me kusht, që të sigurohet një përgjigje e shpejtë dhe efektive për incidenetet e sigurisë si:

Infektimi nga viruse të ndryshme

Hackim

Shperndarja e informacionit konfidencial

Ndërprerje e sistemit të shërbimit

Shkelja e te dhënave personale, etj.

Misioni i ekipit të reagimit është të parandalojë humbjet e mëdha në fitime, humbjen e besimit në publik, apo të dhënave të të tjera duke siguruar një përgjigjë të menjëhershme, të shpjetë dhe efektive për cdo event të papritur. Ai është i autorizuar të ndërmarrë hapat e duhur dhe të nevojshëm për kontrolluar dhe zgjidhur incidentet e sigurisë.

Anëtarët e ekipit te reagimit ndaj incidenteve

Inxhinieri i Telekomunikacionit

Pergjegjesi per rrjetet kompjuterike

Administratori

Shkelja e te dhënave personale

Ky plan i reagimit ndaj incidenteve përshkruan hapat që kompania jonë do të ndërmareë për të zbuluar aksesin e paautorizuar në të dhënat personale të një individi, që mund të rezultojë në dëm, bezdisje, mashtrim apo vjedhje të identititet. Individi mund të jetë një klient ose punonjë i kompanisë.

Informacioni personal është informacion i cili lidhet me të dhëna një individ të identifikueshëm. Pjesa më e madhe e informacionit që kompania mbledh për një individ konsiderohen si të dhëna personale.

Shkelja e sigurisë

Shkelja e sigurisë konsiderohet përvetësimi të dhënave të cilat konpromentojnë sigurinë, konfidencialitetin apo integritetin e të dhënave personale. Përvetësimi në mirëbesim i dhënave personale nga një punonjës i kompanisë për qëllime biznesi nuk është shkelje, me kusht që informacioni personal nuk është përdorur në mënyrë të paautorizuar.

Mbajtesit e te dhenave duhet të identifikojnë dhe të dokumentojnë të gjitha proceset dhe sistemet që ruajnë dhe përdorin të dhënat personale. Të gjithë përdoruesit e autorizuar që mund të hyjnë dhe shfrytëzojnë të dhënat personale janë të identifikueshëm. Identifikimi bëhet përmes emrit të përdoruesit dhe fjalëkalimit të tij unik. Shtimi, fshirja apo ndryshimi i një përdoruesi bëhet nga administratori i sistemit.

Njoftimi i menjëhershëm

Pas ndodhjes së incidenteve të mëposhtme duhet të bëhet menjëherë njoftim

- Një punonjës ka siguruar akses të paautorizuar në të dhëna personale.
- Një person i jashtëm ka thyer sistemin e të dhënave, i cili ka informacion konfidencial.
- Një kompjuter, laptop, CD I cili përmban të dhëna konfidenciale është vjedhur ose ka humbur.

Anëtarët e ekipit të reagimit ndaj incidenteve duhet të mbajnë shënime të sakta për cdo veprim të ndermarrë me orën dhe datën e saktë. Secili person i përfshirë në investigim duhet të regjistroje aksionet që merr përsipër.

Pergjegjësite e mbajtesit te te dhenave.

Mbartësi i të dhënave përgjegjës për të dhënat personale që luajnë një rol aktiv në zbulimin dhe raportimin e çdo shkelje ose shkelje të dyshuar të informacionit mbi një individ. Përveç kësaj, ata do të shërbejnë si një ndërlidhje në mes të kompanisë dhe një pale të tretë të përfshirë me një shkelje të privatësisë ose të dhenave personale. Të gjithë pronarët e të dhënave duhet të raportojnë çdo shkelje të dyshuar ose konfirmuar të

informacionit personal mbi individët pranë KLOBES menjëherë pas evidentimit. Kjo përfshin njoftimin e marrë nga çdo ofrues të shërbimit, parti e tretë apo partnerët e tjerë të biznesit me të cilët ndan organizimit të informacionit personal të individëve. KLOBES do të njoftojë pronarët e të dhënave sa herë që një shkelje ose shkelje të dyshuar të informacionit personal të individëve ndikon në zonën e saj të biznesit.

Sistemet tona monitorohen 24 ore ne dite nga programe kompjuterike monitorimi qe bazohen ne protokolin ICMP. Keto programe njoftojne menjehere me Email nese ka nje problem me lidhjen e sistemeve.

5.2. Raportimi i incidentit dhe komunikimi

Sistemet tona monitorohen 24 ore ne dite nga programe kompjuterike monitorimi qe bazohen ne protokolin ICMP. Keto programe njoftojne menjehere me Email nese ka nje problem me lidhjen e sistemeve.

Menjehere pas marrjes se informacionit ne lidhje me problemin procedohet ne evidentimin e problemit dhe riparimin e menjehershem nepermjet zevendesimit te pjeses difektoze. Pas riparimit te plote te difektit behet diagnostikimi per te gjetur shkakun e detajuar te defektit.

Defektet dhe incidentet rregjistrohen me pas ne protokollet e punes.

VI. Menaxhimi i vazhdimit te biznesit

6.1.Strategjia e Vazhdimit të Shërbimit dhe Planet e Emergjencës

Plani vazhdimit të biznesit lidhet me të gjitha funksionet e biznesit dhe jep ushëzime për mënyrën e reagimit dhe veprimet rimëkëmbëse. Plani vihet në veprim kur:

- Aksesi në një nga centralet është pjesërisht i pamundur për shkak të një incidenti.
- Sistemi i sherbimit te kompanisë është ndërprerë.
- Për cështje të sigurisë së shëndetit të punonjësve dhe klientëve

Plani aplikohet për këto emergjenca:

- Humbje total ose e pjesshme e pajisjeve elektrike
- Përmbytje

- Shpërthim
- Zjarr
- Humbja e sistemeve kritike
- Emergjenca mjekësore

Plani hyn në veprim nëse një incident ndikon në operacionet e biznesit. Anëtarët e ekipit të emergjencës duhet të vendosen në gatishmëri në rast se incidenti cilësohet si faze rreziku 2 dhe duhet të jenë të gatshëm të reagojnë në një faze rreziku 1.

Fazat e aktivizimit të planit të vazhdimit të biznesit

Faza 3 – Nuk ka rrezik të menjëhershëm për sigurinë, por situata emergjente ka ndikim në funksionimin e një nga centralet, që mund të cojë në mbylljen e përkohshme të tyre.

Faza 2 – Jane idetifikuar kërcënime për sigurinë që nuk janë të menjëhershme dhe ka impact të madh në funksionimin e biznesit.

Faza 1 – Kercenim I menjëhershëm I sigurisë së personelit dhe biznesit, e cila shoqërohet me evakuim dhe mbyllje të ndërtesës.

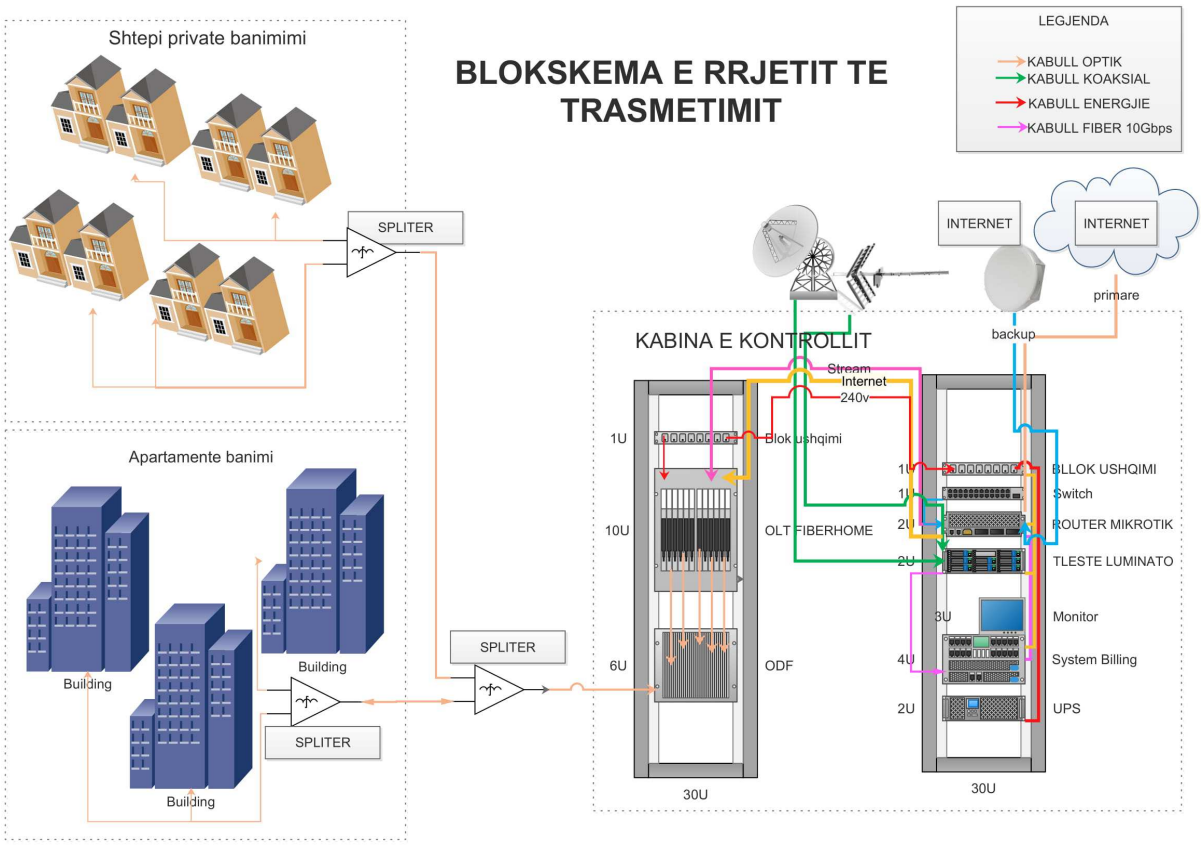
Shkallët e përgjigjes

Nivel 1 - Ndërpreja e funksionimit të përkohshëm te njërit nga centralet për shkak të një defekti në rrjetin elektrik

Niveli 2 – Ndërprerja e aktivitetit të biznesit në një ose më shumë centrale duke përfshirë dy ditë pune dhe zbatimi I planit emergjent do të ndërmerret nga anëtarët e ekpit të emergjencës.

Niveli 3 – Ndërprerja e aktivitetit që ndikon në funksionimin e kompanisë. Një incident natyror i cili do të kërkojë aktivizimin e menjëhershëm të planit të vazhdimsisë së biznesit.

KLOBES Adresa : RRuga “HAMIT DOLLANI”, Prane DSHP Gramsh Tel: 0697007067 e-mail : info@klobes.al



Incidente te kostatuara

nr	Data e kostatimit	Lloji I incidntit	Kohezgjatja	Deme	Shenim
1	18/01/2018	Ushques I radion AP I djegur	1ore	Pervec karikuesit asgje tjeteer	Vendosja e nje karikuesi 24v
2	28/05/2018	Sulm kibernetik ne ruterin kryesor	10min	Rikthim ne gjendje fillestare, dhe restore nga backup e ruajtura me pare, hubje informacioni ska	Routeri I be I pa aksesuashe me kredencialet e ruajtura, mbas rikthimit nga backup caktivizojme portat SSH, FTP, Web, per te evituar perseritjen
3	15/06/2018	UPS Inverter jashte funksioni	5min	Kalimi ne sitem pa bateri (ups off)	Rishimi per ta rivendosur deri ne nje moment sa me shpejt.