Tallinna Ülikool
Informaatika instituut

„Missioonikriitiliste IT-teenuste riskide hindamise mudel“

Magistritöö

Autor: Janno Pugi

Juhendaja: Katrin Niglas

Autor: ..... “.....“ ..... 2008.a.

Juhendaja: ..... “.....“ ..... 2008.a.

Instituudi direktor: ..... “.....“ ..... 2008.a.

Tallinn 2008

Sisukord

1. Sissejuhatus

Teenusehalduritel, kelle üheks kohustuseks on teenuse kvaliteedi parandamine, on vaja saada head ülevaadet missioonikriitilistest IT-teenustest, määratleda nende ohtusid ja hinnata riske.

On olemas palju IT-riskihindamise vahendeid ja mudeleid, kuid kõik nad on mõeldud IT-riskijuhtidele ning on liiga kõike hõlmavad, sisaldades teenusehalduritele palju mittevajalikku. Oleks tarvis vahendit teenusehalduritele IT-teenuste riskide hindamiseks. Kui kõikide teenuste ohud ja riskid on määratletud ühtse mudeli alusel, on hea saada kiiret ülevaadet - näha, mis vajab parandamist, millega on kõik korras, mida tuleks edasiste arenduste ja halduse puhul silmas pidada.

Magistritöö eesmärgiks on uurida erinevaid turvastandardeid, etalonturbe süsteeme ja nendega seonduvaid materjale, et leida sobiv või koostada nende põhjal missioonikriitiliste IT-teenuste nõrkuste määratlemise ja riskide hindamise mudel, mis oleks kasutamiseks eelkõige just teenusehalduritele.

Teenusehalduri all on silmas peetud ITIL'i mõistes *service manager*'i, kes on teenuse omanik, mille läbi pakutakse klientidele väärtusi. Tema ülesandeks on teenuse eest vastutamine, selle juures tehtavate muudatuste aktsepteerimine, suhtlemine äri poolega, raportite esitamine, ...

Magistritöö kontekstis on teenuste all on mõeldud IT missioonikriitilisi teenuseid, mis on suunatud eelkõige välistele kasutajatele - näiteks pankade internetikeskkonnad ja kaardimaksesüsteemid. Seda just eelkõige sellepärast, et missioonikriitilised teenused on ettevõtte ja teenusehalduri jaoks kõige tähtsamad, kuna nende seisaks võib põhjustada suure rahalise või maine kahjustuse.

Magistritöö tulemuseks on lihtsasti kasutatav mudel teenusehalduritele IT missioonikriitiliste teenuste riskide hindamiseks.

2. Mõisted

2.1. Vara (Asset)

Varad on kõik asjad ja ressursid, millel on organisatsiooni jaoks teatud kindel ja oluline väärtus.[4, 3.2]

Infosüsteemide põhilised varad on:[1, lk 12]

- andmed
- infotehniline aparatuur
- andmesidekanalid
- baas- ja rakendustarkvara

Süsteemiga seotud ressursside hulka kuuluvad veel:[1, lk 12]

- organisatsioon - selle struktuur ja funktsionaalsus
- personal
- andmekandjad
- dokumendid
- infrastruktuur - territoorium, rajatised ja kommunikatsioonid

Varade põhilised kolm omadust on: käideldavus(*availability*), terviklikkus(*integrity*) ja konfidentsiaalsus(*confidentiality),* mis peavad vastama kokkulepitud vajalikule tasemele.

Käideldavus (*availability*) tähendab varade takistusteta kättesaadavust volitatud kasutajale ja nende teovõimet. Turvasüsteemid ise ei tohi volitatud kasutajale teha takistusi varade kasutamisel ning nende süsteemide tekitatud ajutised kitsendused peavad olema võimalikult väikesed. Turvameetmete rakendamisel tuleb leida alati optimaalne kompromiss turvalisuse ja kasutusmugavuse vahel. Näiteks hakkavad kasutajad ülemääraselt rangeid turvaeeskirju lihtsalt ignoreerime, otsima võimalusi liiga aeganõudvatest pääsuprotseduuridest möödahiilimiseks jne... [1, lk 13]

Terviklikkus (*integrity)* tähendab, et varasid tohivad muuta ainult volitatud asjaosalised. Muutmine hõlmab kirjutamist, kustutamist, loomist, oleku muutmist jne...[1, lk 13]

Konfidentsiaalsus (*confidentiality)* tähendab, et arvutisüsteemi varad on kättesaadaad ainult volitatud asjaosalistele. [1, lk 13]

Ülejäänud omadused:

Jälitatavus (*Accountability)* omadus, mis tagab, et mingi olemi toiminguid saab üheselt jälitada selle olemini. [4, 3.1]

Autentsus (*Authenticity)* - omadus, mis tagab, et mingi subjekti või ressursi identsus ühtib väidetavaga. Autentsus puudutab kasutajaid, protsesse, süsteeme, informatsiooni jm olemeid. [4, 3.3]

Töökindlus (*Reliability)* - ettenähtud käitumise ja tulemuste järjekindlus. [4, 3.12]

Varade puhul on ka väga oluline, et nad kuuluksid konkreetselt kellelegi, kes nende eest vastutab ja kelle jaoks sisaldavad antud varad väärtusi.

2.2. Nõrkus (Vulnerability)

Nõrkus ehk turvaauk on infosüsteemi nõrk koht või turvadefekt, mille kaudu saavad realiseeruda objekti ähvardavad ohud.[1, lk 43] Nõrkus on eeltingimus selleks, et risk saaks muutuda reaalsuseks.

Nõrkusi saab vähendada kasutades turvameetmeid - seeläbi saab vähendada süsteemi jääkriski.

Aktiivset nõrkuste analüüsi on vaja, et teadvustada ja kinnitada süsteemi turva-olukord ning mõista olemasolevaid nõrkusi.

2.3. Oht (Threat)

Oht on süsteemi või organsatsiooni kahjustada võiva soovimatu intsidendi potentsiaalne põhjus. [4, 3.19]

Varasid ähvardavad paljudesse liikidesse kuuluvad ohud. Ohus peitub võimalus põhjustada soovimatut intsidenti, millest võib tuleneda süsteemi või organisatsiooni ja ta varade kahjustus. Sellise kahjustuse võib põhjustada infotehnoloogilise süsteemi või teenusega töödeldava informatsiooni otsene või kaudne rünne, näiteks informatsiooni volitamatu hävitamine, avalikustamine, muutmine, laostamine ning käideldamatus või kadu. Vara edukaks kahjustamiseks peab oht ära kasutama vara mingi nõrkuse. Ohud võivad pärineda looduslikust või inimallikast ning olla juhuslikud või sihilikud. [4, 8.2]

2.4. Risk (Risk)

Risk on võimalus, et vaadeldav oht kasutab ära mingi vara või vararühma nõrkused, põhjustades varade kaotuse või kahjustuse. [4, 3.14]

IT-turva juhtide kõige suurem eesmärk ongi just riski vähendamine. Riski vähendamiseks tuleb turvaauke lappida turvameetmeid kasutades. Enamasti ei ole kõiki riske võimalik kõrvaldada, kuna see läheks ülearu kulukaks. Tuleb kokkuleppida teatud aktsepteeritav jääkriski tase, arvestades võimalikku mõju ja kulusid.

Riske aktsepteeritakse organisatsioonis, kui need on madalad või ei ole kuluefektiivsed. Riski vähendamiseks kulutatud summa ei tohiks olla suurem, kui riskist tuleneva tagajärje mõju hind ettevõtte jaoks.

2.5. Turvameede (Security measure)

Turvameede on riski kahandav teoviis, protseduur või mehhanism. [4, 3.17]

Turvameetmed võimaldavad vähendada nõrkusi ehk turvaauke ning seeläbi on võimalik vähenda süsteemi jääkriski.

Mitte ühegi turvameetme rakendamine ei anna kunagi täielikkus turvalisust. Need vaid vähendavad (turva)riski, et andmete terviklus, käideldavus või konfidentsiaalsus saavad kahjustatud.

2.6. Toime (Impact)

Toime on tahtliku või juhusliku soovimatu intsidendi tagajärg, mis mõjutab varasid. [4, 3.8]

Tagajärjeks võib olla IT süsteemide rike, konfidentsiaalsuse kadu, terviklikuse või käideldavuse kadu. Võimalikeks kaudseteks kadudeks võib-olla finantsiline kaotus, turuosa kaotus või ettevõtte imago kahjustatus. [4, 84]

2.7. Teenus (service)

Teenus on vahend klientidele väärtuste pakkumiseks. [6, lk 11].

Väärtuse pakkumine on teenuse puhul kõige tähtsam. Klientide jaoks on olulised kaks põhilist asja: kasulikkus/praktilisus ja kindlus ehk mida ja kuidas neile pakutakse. [8, lk 16]

2.8. Teenusehaldur (service manager)

Teenusehaldur tegeleb teenus(t)e haldamisega, mis sisaldab endas teenuste tundmist, teenusega seotud rakenduste haldust, suhtlemist äri poolega, teenuse kvaliteedi parandamist, muudatuste aktsepteerimist, ülevaate omamist IT võimaluste kohta, ... [7, 3.1]

Teenusehaldur kuulub teenustehalduse(*service management*) koosseisu.

ITIL defineerib teenustehaldust kui organisatsiooni spetsiaalseid võimalusi pakkumaks klientidele väärtusi läbi teenuste. [8, lk 16]

3. Missioonikriitiliste teenuste tunnused

Missioonikriitiliste teenuste mõiste tähendus varieerub kindlasti erinevates ettevõtetes.

Antud magistritöö raames on missioonikriitiliste teenuste all silmas peetud selliseid teenuseid, millede seisak põhjustab ettevõttele suure rahalise kahju (näiteks saamata jäänud tulu) või ettevõtte maine väga suure kahjustumise. Viimast võib lugeda rahalisest kahjust isegi palju olulisemaks.

Selliste teenuste puhul on ettevõttele oluline nende väga kõrge käideldavus (*high availability*).

Lähtuvalt ISKE'st, oleks nendeks teenusteks teenused, mis kuuluvad ISKE käideldavuse klassidesse **K2 – töökindlus – 99%** (lubatud summaarne seisak nädalas ~ 2 tundi) ja **K3 - töökindlus - 99,9%** (lubatud summaarne seisak nädalas ~ 10 minutit).

Teenuse taseme lepingute (*Servie Level Agreement - SLA*) sõlmimisel määratakse teenuse tööaeg, maksimaalne lubatud taasteaeg, maksimaalne andmekadu, jne. Missioonikriitilised teenused peavad olema reeglina võimalikult kiiresti taastatavad ja ilma võimaliku andmekaota.

Käesoleva magistritöö raames on missioonikriitiliste teenuste all eelkõige silmas peetud selliseid teenuseid, milledel on olemas väline lõppkasutaja. Sellisteks teenusteks on näiteks: pankade internetikeskonnad, pankade kaardimaksesüsteemid ja tellerite kliendihaldusprogrammid - nende teenuste pikem seisak tööajal põhjustab kindlasti ettevõttele rahalise või manine kahjustuse.

4. Enimkasutatavad infoturbe standardid

Kuna magistritöö eesmärgiks on leida või koostada sobiv mudel missioonikriitiliste IT-teenuste riskide määratlemiseks ja hindamiseks, mis oleks kasutamiseks eelkõige just teenusehaldurtele, siis selleks on uuritud erinevaid turvastandardeid, etalonturbesüsteeme ja nendega seotud materjale.

Kuna loodav mudel on mõeldud põhiliselt teenusehalduritele, siis sellest tulenevalt on rõhk rohkem käideldavusel ja ka terviklusel, kuid mitte konfidentsiaalsusel, kuna see ei ohusta otseselt teenuste stabiilsust või kättesaadavust ning jääb pigem IT-riskijuhtimise valdkonda.

Seega on jäänud ka välja valimata nõuanded, nõrkused ja ohud, mis on seotud konfidentsiaalsusega ning eriti oluliseks on peetud neid, mis võivad olla seotud just käideldavuse ja terviklusega ning seda teenusehalduri vaatevinklist, kuna tema põhiliseks huviks on teenuste stabiilsus.

Vastavad valikud on tehtud autori hinnangul ja IT-teenustehalduses töötamise kogemusel.

Kuna käesoleva magistritöö raames on missioonikriitiliste teenuste all eelkõige silmas peetud selliseid teenuseid, milledel on olemas väline lõppkasutaja, siis sellest lähtuvalt on tehtud ka valikud nõuannete, nõrkuste ja ohtude suhtes.

Magistritöö raames on uuritud enimkasutatavaid infoturbe standardeid:

- Infosüsteemide kolmeastmeline etalonturbe süsteem - ISKE
- The Standard of Good Practice for Information Security (ISF)
- ISO / IEC 17799:2005

Iga materjali puhul on välja toodud mudeli loomise jaoks olulisteks osutunud punktid ning ära on ka mainitud iga kategooria puhul antud magistritöö kontekstis mittevajalikud ohud, nõrkused ja meetodid teenusehalduritele.

4.1. Infosüsteemide kolmeastmeline etalonturbe süsteem - ISKE

ISKE on infosüsteemide kolmeastmeline etalonturbe süsteem. Infovarad on kirjeldatud tüüpmoodulite abil ning iga tüüpmooduli(ohu) puhul määratakse turvameetmed vastavalt vajalikele turvaastmetele.

ISKE põhineb Saksamaa Infoturbeameti (Bundesamt für Sicherheit in der Informationstechnik, BSI) poolt publitseeritaval IT etalonturbe käsiraamatul (IT Grundschutzhandbuch'il). BSI süsteem on väga ulatuslikult ja detailselt dokumenteeritud ning seda täiendatakse regulaarselt kord aastas. [2, lk 10]

ISKE on mõeldud andmekogude pidamisel kasutatavate infosüsteemide ja nendega seotud infovarade turvalisuse saavutamiseks ja säilitamiseks. ISKE on rakendatav ka muudes riigi- ja omavalitsusasutustes, äriettevõtetes ja mittetulunduslikes organisatsioonides. [2, lk 7]

Ohud on liigitatud ISKES kuude kategooriasse: [2, lk 181]

1. Vääramatud jõud
2. Organisatsioonilised puudused
3. Inimvead
4. Tehnilised rikked ja defektid
5. Ründed
6. Andmekaitseohud

4.1.1. Vääramatud jõud

Teenusehalduri jaoks olulised:

- Personali väljalangemine (haigus, õnnetus, surm, streik, lahkumine)

Vääramatute kategooria sisaldab veel lisaks ohtusid nagu näiteks: IT-süsteemi avarii(tehnilise rikke, inimvea, vääramatu jõu vms tõttu), äike, kahjutuli, vesi, tugevad magnetväljad, andmete kadu tugeva valguse toimel, keskkonna õnnetused.

4.1.2. Organisatsioonilised puudused

Teenusehalduri jaoks olulised:

- Tarkvara testimis- ja evitusprotseduuride puudumine või puudulikkus
- Dokumentatsiooni puudumine või puudulikkus (konfiguratsiooni muutused, tõrkeotsing)
- Liini piisamatu ribalaius (võrgu plaanimine tulevikuvaruta)
- Andmebaasi turvamehhanismide puudumine või puudulikkus (paroolid jms)
- Registreerimata komponentide kasutamine
- Halb väljasttellimise strateegia
- Sõltuvus välisest teenusetarnijast

Organisatsiooniliste puuduste kategooria sisaldab veel lisaks ohtusid nagu näiteks: volitamatu pääs ruumidesse, kaablite puudulik dokumenteerimine, sülearvuti reguleerimata edasiandmine, andmekandjate puudulik märgistus, faksimaterjalide ebapiisav varu, volitamatu isikuandmete kogumine, ebapiisav traadita kohtvõrgu kontroll, failide ja andmekandjate ebaturvaline transport, halb krüpteerimise korraldus, liinide väike läbilaskevõime, ressursside kontrollimatu kasutamine.

4.1.3. Inimvead

Teenusehalduri jaoks olulised ():

- Seadme või andmete hävitamine kogemata
- IT-süsteemi väär haldus (väär installeerimine, pääsuõiguste liiga lõtv jagamine, logi ei kasutata)
- Väär pääsuõiguste haldus (võimalus kustutada logiandmeid, ebapiisav ligipääs oma töö tegemiseks)
- Andmebaasisüsteemi hooletu haldus (liigsed õigused, seire puudumine, harv varukopeerimine)
- Sündmuste väär tõlgendamine (süsteemihalduses: valealarmid jms)
- Vead konfigureerimisel ja opereerimisel

Inimvigade kategooria sisaldab ka lisaks ohtusid nagu näiteks: lubamatud kaabliühendused, koristajad jm väljastpoolt töötajad, väär sendmaili konfigureerimine, automaatvastaja väär käsitsemine, mehaaniliste koodlukkude võtmete väär kasutamine, tulemusteta otsingud, vead Lotus Notes serveri konfigureerimisel, Tuletõkete kahjustamine.

4.1.4. Tehnilised rikked ja defektid

Teenusehalduri jaoks olulised:

- Sisevõrkude katkestus
- Programmivigade ilmnemine
- Andmebaasi väljalangemine (riistvara tõrke, ründe vm tõttu)
- Andmete kadu andmebaasis (kogemata, rünne, rike,...)
- Andmete kadu andmebaasis, salvestusruumi puudumise tõttu
- Võrgu- või süsteemihaldussüsteemi komponendi tõrge
- Dokumenteerimata funktsioonid (eriti rakendusprogrammides: nt tagauksed)
- Välise teenusetarnija süsteemide tõrge

Tehniliste rikete ja defektide kategooria sisaldab veel lisaks ohtusid nagu näiteks: liinihäired keskkonna toimel, läbikoste, faksi termopaberi riknemine, automaatvastaja avariipatarei tühjenemine, tasandusvoolud varjes, Novell eDirectory tõrge, raadiolainete kontrollimatu levi, ebapiisav pistikupesade arv, tolmused ventilaatorid, toitevõrgu katkestused, IP-kõne arhitektuuri väljalangemine, IP-kõne terminalide nõrkused.

4.1.5. Ründed

Rünnete kategoorias olevad ohud võivad kõik mõjutada süsteemi ja teenuste stabiilsust ning käideldavust, kuid nende ohtude näol ei ole otseselt tegemist teenusehalduri haldushalasse jäävate probleemidega.

Kuid teenusehaldur peab olema vähemalt teadlik sellest, mil moel võivad tema teenused rünnatavad olla.

Rünnete kategooria sisaldab näiteks ohtusid: IT-seadmete või -tarvikute manipuleerimine või hävitamine, andmete või tarkvara manipuleerimine (vale sisestus, pääsu muutumine), sisekeskjaamas salvestatud andmete leke, volitamatu sisenemine hoonesse, vargus, vandalism, telefonikõnede ja andmesaadetiste pealtkuulamine, pealtkuulamine ruumides, uudishimulik töötaja, andmekandjate volitamata kopeerimine, andmete/tarkvara manipuleerimine andmebaasisüsteemis, meilipommid, mobiilkõnede pealtkuulamine, sabotaaž, MAC-aadresside võltsimine, andmekappide sihilik väärkasutus mugavuspõhjustel (koodluku lahtijätmine), sihilik väärkonfiguratsioon,...

4.1.6. Andmekaitseohud

Teenusehalduri jaoks olulisi ohte see kategooria ei sisalda, kuna antud ohud ei mõjuta otseselt teenuse käideldavust, kuid teenusehaldur peab olema kindlasti teadlik erinevatest andmekaitseohtudest.

Andmekaitseohtude kategooriasse kuuluvad näiteks ohud: puuduvad või piisamatud õiguslikud alused, sihipärasuse rikkumine, teadmisvajaduse printsiibi rikkumine, andmesaladuse rikkumine, asjasse puutuvate isikute õiguste rikkumine, läbipaistmatus asjasse puutuvaile ja andmekaitse kontrolliorganitele, etteantud kontrolleesmärkide ohustamine, puuduv või piisamatu andmekaitse kontroll.

4.2. The Standard of Good Practice for Information Security

„The Standard of Good Practice for Information Security“ on koostatud rahvusvahelise assotsatsiooni Information Security Forum (ISF) poolt. [5, lk 2]

Antud standard sisaldab parimaid praktikaid informatsiooni turvalisusest ja seda uuendatakse regulaarselt. [5, lk 2]

Standard on suunatud informatsiooni turvalisuse juhtidele, äri juhtidele, IT juhtidele, IT audiitoritele, välistele teenusepakkujatele. [5, lk 6]]

Standard toob välja nõuanded, mis on jaotatud kuude kategooriatesse: [5, lk 14]

1. Riskijuhtimine *(Security management)*
2. Kriitilised ärirakendused *(Critical business applications)*
3. Arvutite installatsioon *(Computer Installations)*
4. Võrgud *(Networks)*
5. Süsteemi arendus *(System Development)*
6. Lõppkasutaja keskkond (*End User Environment*)

4.2.1. Riskijuhtimine

Antud kategoorias on teenusehalduri jaoks olulised punktid:

Omamine - kriitilisel informatsioonil ja süsteemidel peab olema vastutav isik, kelle kohustused on selgelt defineeritud ja aktsepteeritud.

Väljasttellimine - väliste tarnijate poolt tehtud süsteemid peavad vastama turvanõuetele.

Kolmandate osapoolte ligipääsetavus - välised ühendused partnerite ja klientidega peavad olema identifitseeritud ja aktsepteeritud.

Riskijuhtimise kategoorias on veel näiteks: turvapoliitikad, kohapealne turva koordineerimine, turva järeleandmised, informatsiooni riski analüüs, turva arhitektuur, varade haldus, füüsiline turve, äri jätkusuutlikus, viiruste tõrje, turvapaikamine, krüptograafia kasutamine, avaliku võtme infrastruktuur, e-mail, turvaseire.

4.2.2. Kriitilised ärirakendused

Antud kategoorias on teenusehalduri jaoks olulised punktid:

Rollid ja vastutused - rakendusel peab olema omanik ja vastutused tähtsamate toimingute tegemiseks määratud individuaalselt.

Muudatuste haldus - muudetavat rakendust peab testima, üle vaatama ja rakendama vastavalt muudatuste halduse protsessile.

Intsidentide haldus - kõik intsidendid peavad saama salvestatud, üle vaadatud ja lahendatud kasutades intsidentide haldamise protsessi.

Äri jätkusuutlikus - ära jätkusuutlikuse plaan peab olema välja töötatud ja testitud regulaarselt.

Teenuste lepingud - arvutid ja võrgud, mis on vajalikud vastava teenuse toetuseks peavad olema teenuse pakkujalt, kes suudavad pakkuda piisavat turvalisust ning kellega on sõlmitud teenuse taseme lepingud.

Elastsus - rakendus võiks töötada töökindlalt ja usaldusväärselt riistvaral ja tarkvaral, mis on duubeldatud.

Välised ühendused - kõik välised ühendused rakendusega peaksid olema määratletud, kontrollitud ja kinnitatud teenuse omaniku poolt.

Varundus - tagavarakoopiate tegemine regulaarselt olulisest informatsioonist ja tarkvarast, mida rakendus kasutab.

Antud kategooria sisaldab lisaks veel näiteks: konfidentsiaalsuse nõuded, sensitiivne informatsioon, töökoha konfiguratsioon, kohalik turvakoordineerimine, informatsiooni riski analüüs, turvaaudit,

avaliku võtme infrastruktuur.

4.2.3. Arvutite installatsioon

Antud valdkond ei ole otseselt seotud teenuse ohtude või nõrkustega, vaid teenuse haldamise vahenditega - kasutajate arvutitega.

Antud kategoorias on teenusehalduri jaoks olulised punktid:

Sündmuste logimine - tegevuste salvestamine

Elektritoide - kriitilised teenused peavad olema kaitstud elektrivoolu katkestuste vastu.

Alternatiivne töökorraldus - alternatiivne töökorralduse plaani olemasolu, testimine ja vajadusel rakendamine

Kategooria sisaldab veel ka näiteks punkte: füüsiline ligipääsetavus, arvutite konfiguratsioon, muudatuste haldus, kasutaja autentimine, informatsiooni riski analüüs.

4.2.4. Võrgud

Antud kategoorias on teenusehalduri jaoks olulised punktid:

Võrgu disain - võrk peab hakkama saama praeguse ja tulevase ennustatava liikluse ja andmemahtudega.

Võrgu monitooring - võrgu aktiivsust peab monitoorima.

Kategooria sisaldab veel ka lisaks: võrguseadmete seadistamine, tulemüürid, juhtmevaba ligipääs.

4.2.5. Süsteemide arendus

Antud kategoorias on teenuse halduri jaoks olulised punktid:

Arenduse poolsed rollid ja vastutused - Et oleks ka teada, kes arenduse poolelt on antud toote omanik, et vajadusel probleemidega tema poole pöörduda.

Testimine - kõiki süsteemi elemente tuleb testida enne kui nad lähevad toodangu keskkonda, võimalikult sarnases keskkonnas.

Süsteemi edutamise kriteeria - Süsteem peab vastama karmidele tingimustele enne kui läheb toodangu keskkonda.

Installeerimine - uute süsteemide installeerimine peab käima kooskõlas dokumenteeritud installeerimise protsessiga.

Kategooria sisaldab ka veel punkte: arenduskeskkond, arendusmetoodikad, informatsiooni riski analüüs.

4.2.6. Lõppkasutaja keskkond

Antud kategoorias on teenuse halduri jaoks olulised punktid:

Rollid ja vastutused - lõppkasutaja keskkonnal peab olema omanik ja võtmeülesanded peavad olema määratud konkreetsetele isikutele.

Turvateadlikkus - Kasutajatele peab olema teadvustatud ohtusid ja vastutust

Kasutajate koolitus - kasutajatele peab olema õpetatud, kuidas töötada süsteemidega korrektselt

Sisselogimis protsess - enne töötamist rakendustega, peab toimuma sisselogimine

Andmebaasi kaitse - rakenduste poolt kasutatav andmebaas peab olema kaitstud

Tagavara koopiad - tähtsat informatsiooni ja tarkvara tuleb varundada

Kategooria sisaldab ka veel punkte: informatsiooni klassifikatsioon, muudatuste juhtimine, rakenduste inventuur, rakenduste arendamine, tööjaamade kaitse, käsiseadmete kaitse, e-mail, internetti pääs, sõnumivahetus, juhtmevaba pääs, füüsiline keskkonna kaitse.

4.3. ISO / IEC 17799:2005

ISO/IEC 17799:2005 „Information technology - Security techniques - Code of practice for information security management“ annab juhised, nõuanded ja üldised põhimõtted informatsiooni turvalisuse parendamiseks ning juhtimiseks organisatsioonis. Antud standard sisaldab parimaid praktikaid ja põhilisi juhtnööre informatsiooni turvalisuse juhtimiseks..

Standard on valmistatud Joint Technical Committee JTC 1, *Information technology,* Subcommittee SC 27, poolt.[3, lk vii]

Antud standard sisaldab kategooriaid:

1. Turvapoliitika
2. Organisatsioon ja informatsiooni turvalisus
3. Varade haldus
4. Inimressursside turvalisus
5. Füüsiline ja keskkonna turvalisus
6. Kommunikatsioonid ja operatsioonide haldus
7. Juurdepääsukontroll
8. Informatsiooni süsteemide omandamine, arendamine ja haldamine
9. Informatsiooni turvalisuse intsidentide haldus
10. Äri jätkusuutlikuse haldus
11. Vastavus

4.3.1. Turvapoliitika

Antud kategoorias teenusehaldurit otseselt puudutavaid punkte ei ole, kuid teenused peavad olema

vastavuses organisatsiooni turvapoliitikaga ning ka teenusehaldur peab selle eest hoolitsema.

Kategooria sisaldab näiteks punkte: informatsiooni turvapoliitika dokumendi olemasolu, informatsiooni turvapoliitika ülevaatus.

4.3.2. Organisatsioon ja informatsiooni turvalisus

Antud kategoorias teenusehaldurit otseselt puudutavaid punkte ei ole.

Kategooria sisaldab näiteks punkte: juhtkonna kohustus toetada informatsiooni turvalisust, informatsiooni turvalisuse koordineerimine, autoriseeritud protsess informatsiooni töötlemiseks, konfidentsiaalsuse lepingud, ühendus juhtkonnaga, ühendust huvigruppidega, väliste osapooltega seotud riskide identifitseerimine.

4.3.3. Varade haldus

Teenusehalduri jaoks oluline punkt:

Varade omanik - kogu informatsioon ja varad, mis on seotud informatsiooni töötlevate seadmetega, peavad kuuluma kellelegi, kes nende eest otseselt vastutab ning esitab nõuded.

Kategooria sisaldab veel ka näiteks punkte: varade inventuur, aktsepteeritud varade kasutamine, informatsiooni liigitus, informatsiooni märgistamine ja hooldamine.

4.3.4. Inimressursside turvalisus

Teenusehalduri jaoks olulised punktid:

Rollid ja vastutus - töötajate rollid ja vastutused peavad olema määratud, samuti kolmandate osapoolte kontaktid.

Kategooria sisaldab veel ka näiteks punkte: taustauuring, töötaja lepingutingimused, informatsiooni turvalisuse koolitus ja õpe, distsiplinaarne protsess, töölepingu lõpetamine, varade tagastamine, sisenemisõiguste eemaldamine.

4.3.5. Füüsiline ja keskkonna turvalisus

Antud kategoorias teenusehaldurit otseselt puudutavaid punkte ei ole.

Kategooria sisaldab näiteks punkte: füüsilise turvalisuse perimeeter, füüsilised sisenemise kontroll mehhanismid, kontorite, ruumide, seadmete turvamine, välimiste ja keskkonna ohtude vastu kaitsemine, töötamine turvalistel aladel, avalik pääsla, varustuse turvalisus, toetavad teenused (toide), kaablite turvalisus, varustuse korrashoid.

4.3.6. Kommunikatsioonid ja operatsioonide haldus

Teenusehalduri jaoks olulised punktid:

Operatsioonide dokumenteerimine - oleks ka teistel teada, kuidas teatud protseduuride tegemine täpsemalt käib.

Muudatuste juhtimine - informatsiooni töötluses ja süsteemides muudatuste tegemine peab olema kontrollitud.

Teenuste tarne kolmanda osapoole poolt - Organisatsioon peab kontrollima implementeerimise lepinguid ja haldama muudatusi, et kindlustada, et teenused vastaksid kokkulepitud nõuetele.

Seire ja ülevaade kolmanda osapoolte teenustele/raportitele - Teenuseid ja raporteid tuleb regulaarselt jälgida ja üle vaadata.

Süsteemide aktsepteerimine - Peab olema kindel, et nõuded uutele süsteemidele on selgelt defineeritud, kokku lepitud, dokumenteeritud ja testitud.

Back-up - Tagavarakoopiate tegemine informatsioonist ja tarkvarast ning selle testimine.

Süsteemi dokumentatsioon - Süsteemi dokumentatsiooni olemasolu ja kaitse.

Logimine ja logide kaitsemine - kasutajate ja süsteemi tegevuse logimine

Seire - süsteemi seire

Süsteemi administraatori ja operaatori logimine - süsteemi administraatori tegevuse logimine

Vigade logimine - süsteemis esinevate vigade logimine

Kategooria sisaldab veel ka punkte: mahtude haldus, kontrolli teostamine ründeprogrammikoodide vastu, võrkude kontroll, turvalised võrgu teenused, kõrvaldatavad andmekandjad, andmekandjate hävitamine/kõrvaldamine, informatsiooni käsitsemise protseduurid, informatsiooni vahetamise poliitikad ja protseduurid, füüsiliste andmekandjate transport, elektrooniline sõnumivahetus, avalik informatsioon.

4.3.7. Juurdepääsu kontroll

Teenuse halduri jaoks olulised punktid:

Privileegide haldus - rakenduses privileegide (eriõiguste) kasutamine peab olema piiratud ja kontrollitud.

Võrkude eraldamine - erinevate teenuste võrkude eraldamine

Kategooria sisaldab veel ka näiteks punkte: kasutaja paroolide haldus, tühja laua poliitika, võrgu juurdepääsu kontroll, võrguteenuste kasutamise poliitika, kaugdiagnostika ja seadistuspordi kaitse, võrguühenduste kontroll, võrgu suunamise kontroll, operatsioonisüsteemide sisenemise kontroll, paroolihaldussüsteemid, ühenduse ajalimiit, sensitiivsete süsteemide isolatsioon, mobiilne arvutamine ja ühendused.

4.3.8. Informatsiooni süsteemide omandamine, arendamine ja haldamine

Teenusehalduri jaoks olulised punktid:

Sisendandmete kontroll - Andmete kontroll enne andmete töötlust

Sisemiste protsesside kontroll - Sisemiste protsesside jälgimine, et avastada töötlemise käigus tekkinud rikutud informatsiooni.

Väljundandmete kontroll - Väljundandmete kontrollimine, et töödeldud ja salvestatud andmed oleksid õiged.

Muudatuste kontroll - Implementeeritavaid muudatusi tuleb kontrollida vastavalt protseduuridele.

Väljastellitud tarkvara - Väljasttellitud tarkvara jälgmine ja kontrollimine

Kategooria sisaldab ka veel punkte: turvanõuete analüüs ja spetsifikatsioon, krüptograafia vahendite kasutamise poliitika, võtmete haldus, operatsiooni tarkvara kontroll, testandmete kaitse, programmikoodi kaitse, tarkvara pakettides muudatuste tegemise piiramine, informatsiooni lekkimine.

4.3.9. Informatsiooni turvalisuse intsidentide haldus

Teenusehalduri jaoks olulised punktid:

- **Informatsiooni turvalisuse sündmustest raporteerimine** - raportite koostamine ja esitamine
- **Turvanõrkustest raporteerimine** - olla teadlik oma süsteemi nõrkustest/vigadest

Kategooria sisaldab näiteks punkte: vastutajad ja protseduurid, informatsiooni turvalisuse intsidentidest õppimine, tõendite kogumine.

4.3.10. Äri talituspidevuse haldus

Antud kategoorias teenusehaldurit otseselt puudutavaid punkte ei ole, kuid teenusehaldur peaks olema kursis ka äri poolse talituspidevuse plaanidega.

Kategooria sisaldab näiteks punkte: informatsiooni turvalisuse sidumine äri talituspidevuse halduse protsessiga, äri talituspidevus ja riski hindamine, talituspidevuse plaanide arendamine ja rakendamine kaasates informatsiooni turvalisust, äri talituspidevuse planeerimise raamistik, äri talituspidevuse plaanide testimine, hooldamine ja hindamine.

4.3.11. Vastavus

Antud kategoorias teenusehaldurit otseselt puudutavaid punkte ei ole.

Kategooria sisaldab näiteks punkte: intellektuaalse omandi õigused, organisatsiooniliste salvestiste kaitse, andmete ja personali privaatsuse kaitse, informatsiooni töötlevate seadmete vale kasutamise ärahoidmine, krüptograafiliste vahendite regulatsioon, turvapoliitikate, standardite ja tehniline valmisolek, informatsiooni süsteemide auditi läbivaatlus, auditi vahendite kaitse.

5. Teenusehaldurile oluliste riskide liigitus

Kuna riskide määratlemist ja hindamist teostatakse põhiliselt ikka selleks, et neid hiljem maandama hakata, siis on ka oluline teada riskide allikat. Ehk näiteks, kas muresid põhjustavad riskid tulenevad näiteks personalist või tehnikast või hoopis valest ja vigasest töökorraldusest.

Seega, autori arvates on kolm põhilist kategooriat, mis puudutavad otseselt teenusehaldurit ja mille alla on ka edaspidises kõik eelmises peatükis välja valitud nõuanded, nõrkused ning ohud ära jaotatud:

1. Personal
2. Protsessid
3. IT ja süsteemid

Antud riskide liigitus on aluseks soovitud mudeli loomiseks ja töö eesmärgi saavutamisele.

Kui mitmes materjalis/allikas on käsitletud samu nõrkusi, ohtusid või nõuandeid, siis siin on nad koondatud ühe punkti alla. Iga punkti taha on lisatud algallikas (ISKE, ISO 1779 ja ISF ehk The Standard of Good Practice).

Kuna vaadeldud materjalid on sisaldanud lisaks nõrkustele ka ohtusid ja lihtsalt turvameetmeid, siis siin on iga punkti juures autori poolt ära toodud konkreet(sed)ne nõrkus(ed) ning võimalik oht, mis võib seda nõrkust ära kasutada.

Lisatud on ka punktid ja nõrkused, mida ei leidunud uuritavates materjalides, kuid mis peaksid autori teenustehalduses saadud töökogemuse põhjal kuuluma veel lisaks nende kategooriate alla.

5.1. Personal

Personali riskid on seotud eelkõige inimeste teadmistega, käitumisega, kontakteerumisega, kättesaadavusega, ...

- **Personali väljalangemine** (haigus, õnnetus, surm, streik, lahkumine) - ISKE
  Nõrkus: Kompetentse personali vähene töövalmidus/dubleerimatus
  Oht: Kriitilises situatsioonis puudub tugi kompetentse personali poolt (näiteks süsteemi administraatorite)

- **Seadme või andmete hävitamine kogemata** - ISKE;
  Nõrkus: Personali teadmatus või lohakus andmetega ümber käimisel
  Oht: Seadme või andmete hävitamine kogemata

- **Operatsioonid sisaldavad suurel hulgal käsitsitegevusi**
  Nõrkus: Operatsioonid sisaldavad suurel hulgal käsitsitegevusi
  Oht: Operatsioonid aeganõudvad, andmete hävitamine kogemata, käideldavuse/tervikluse kadu

- **Vead konfigureerimisel ja opereerimisel** - ISKE; **IT-süsteemi väär haldus** (väär installeerimine, pääsuõiguste liiga lõtv jagamine) - ISKE
  Nõrkus: Ebakompetentne personal (konfigureerimine, IT-süsteemi haldus)
  Oht: Tehakse vigu süsteemide konfigureerimisel ja opereerimisel/haldamisel, mille tulemuseks võib olla näiteks käideldavuse või tervikluse kadu

- **Sõltumine (välistest) konsultantidest**
  Nõrkus: Sõltumine (välistest) konsultantidest
  Oht: Kriitilises situatsioonis peab pöörduma abi saamiseks välise konsultandi poole, kes võib olla kättesaamatu ning probleemi lahendamine võtta väga palju aega

- **Kasutajate koolitus** - kasutajatele peab olema õpetatud, kuidas töötada süsteemidega õigesti - ISF
  Nõrkus: Kasutajaid ei tööta süsteemidega õigesti
  Oht: Võimalik käideldavuse, tervikluse või konfidentsiaalsuse kadu

- **Informatsiooni turvalisuse sündmustest raporteerimine** - raportite koostamine ja esitamine
  Nõrkus: Turvaintsidentidest raporteerimine puudub või on puudulik
  Oht: Intsidendid võivad korduda

- ***Turvanõrkustest raporteerimine*** - olla teadlik oma süsteemi nõrkustest/vigadest
  Nõrkus: Turvanõrkusetele ei pöörata tähelepanu
  Oht: Turvanõrkustele tähelepanu pööramata võib toimuda käideldavuse, tervikluse või konfidentsiaalsuse kadu

5.2. Protsessid

Protsesside riskid on seotud eelkõige ettevõtte töökorraldusega ja sellega seonduvaga.

- **Omamine** - Kriitilisel informatsioonil ja süsteemidel peab olema vastutav isik, kelle kohustused on selgelt defineeritud ja aktsepteeritud - ISF; **Varade omanik** - kogu informatsioon ja varad, mis on seotud informatsiooni töötlevate seadmetega, peavad kuuluma kellelegi, kes nende eest otseselt vastutab - ISO 17799; **Registreerimata komponentide kasutamine** - ISKE
  Nõrkus: Informatsioonil või süsteemil puudub omanik
  Oht: Kriitilises situatsioonis pole teada, kes süsteemi eest vastutab ja seega võib tema leidmine võtta väga palju aega.

- **Rollid ja vastutused** - rakendusel peab olema omanik ja vastutused tähtsamate toimingute tegemiseks määratud individuaalselt - ISF; **Rollid ja vastutus** - töötajate rollid ja vastutused peavad olema määratud, samuti kolmandate osapoolte kontaktid - ISO 17799; **Arenduse poolsed rollid ja vastutused** - Et oleks ka teada, kes arenduse poolelt on antud toote omanik, et vajadusel probleemidega tema poole pöörduda - ISF
  Nõrkus: Töötajate rollid ja vastutused pole täpselt määratletud
  Oht: Kriitilises situatsioonis ei ole teada, kes peaks antud probleemiga tegelema
  Nõrkus: Arenduse poolsete kontaktide ja vastutajate puudumine
  Oht: Kriisi situatsioonis pole täpselt teada, kelle poole arendusest abi saamiseks pöörduda ning selle väljaselgitamine võib võtta väga palju aega.

- **Väär pääsuõiguste haldus** (võimalus kustutada logiandmeid, ebapiisav ligipääs oma töö tegemiseks) - ISKE
  Nõrkus: Ebapiisav ligipääs töö tegemiseks
  Oht: Pole võimalik kiiresti teenuse stabiilsust päästa (näiteks puudub ligipääs logidele)
  Nõrkus: Liigne pääs töö tegemiseks
  Oht: Teenuse stabiilsuse ohustamine (kogemata peatamine vms)

- **Tarkvara testimis- ja evitusprotseduuride puudumine või puudulikkus** - ISKE; **Testimine** - kõiki süsteemi elemente tuleb testida enne kui nad lähevad toodangu keskkonda, võimalikult sarnases keskkonnas - ISF; **Programmivigade ilmnemine** - ISKE
  Nõrkus: Tarkvara testimine viiakse läbi puudulikult
  Nõrkus: Tarkvara testimine viiakse läbi toodangu keskkonnast erinevas keskkonnas
  Oht: Toodangu süsteemides ehk reaalses kasutuses ilmnevad (kriitilised) vead

- **Dokumentatsiooni puudumine või puudulikkus** - ISKE; **Süsteemi dokumentatsioon** - Süsteemi dokumentatsiooni olemasolu ja kaitse - ISO 17799; **Operatsioonide dokumenteerimine** - oleks ka teistel teada, kuidas teatud protseduuride tegemine täpsemalt käib - ISO 17799; **Dokumenteerimata funktsioonid** (eriti rakendusprogrammides: nt tagauksed) - ISKE

Nõrkus: Süsteemi ja/või operatsioonide kohta puudub korralik dokumentatsioon
Oht: Süsteemi hallatakse või administreeritakse vigaselt/puudulikult

- **Muudatuste haldus** - muudetavat rakendust peab testima, üle vaatama ja rakendama vastavalt muudatuste halduse protsessile - ISF; **Muudatuste juhtimine** - informatsiooni töötluses ja süsteemides muudatuste tegemine peab olema kontrollitud - ISO 17799; **Muudatuste kontroll** - Implementeeritavaid muudatusi tuleb kontrollida vastavalt protseduuridele - ISO 17799;
  Nõrkus: Muudatuste tegemine süsteemides ei ole kontrollitud
  Oht: Süsteemid muutuvad kontrollimatult, võivad muutuda ühildamatuteks ja ebastabiilsemateks. Rakenduse tagasirullimine võib olla plaani puudumise tõttu raskendatud.

- **Süsteemide aktsepteerimine -** Peab olema kindel, et nõuded uutele süsteemidele on selgelt defineeritud, kokku lepitud, dokumenteeritud ja testitud - ISO 17799; **Süsteemi aktsepteerimise kriteeria -** Süsteem peab vastama kõikidele esitatud tingimustele enne kui läheb toodangu keskkonda - ISF
  Nõrkus: Nõuded uutele süsteemidele ebaselged, defineerimata
  Oht: Toodangusse satub süsteem, mis ei vasta nõuetele ja vajadustele

- **Intsidentide haldus** - kõik intsidendid peavad saama salvestatud, üle vaadatud ja lahendatud kasutades intsidentide haldamise protsessi - ISF
  Nõrkus: Intsidentide haldus puudub või on puudulik
  Oht: Puudub teadmine ega teki arusaama, kuidas hoida ära tulevikus analoogseid intsidente

- **Jätkusuutlikus** - jätkusuutlikuse plaan peab olema välja töötatud ja testitud regulaarselt - ISF
  Nõrkus: Taasteplaan puudub, on puudulik või testimata

Oht: Puudub ülevaade, kuidas teenuse taastamine peaks toimuma ning see võtab väga kaua aega.

- **Teenuste lepingud** - arvutid ja võrgud, mis on vajalikud vastava teenuse toetuseks peavad olema teenuse pakkujalt, kes suudavad pakkuda piisavat turvalisust ning kellega on sõlmitud teenuse taseme lepingud - ISF
  Nõrkus: Teenuste taseme lepingud puuduvad
  Oht: Teenust ei pakuta piisaval tasemel

- **Teenuste tarne kolmanda osapoole poolt** - Organisatsioon peab kontrollima implementeerimise lepinguid ja haldama muudatusi, et kindlustada, et teenused vastaksid kokkulepitud nõuetele - ISO 17799; **Väljastellitud tarkvara** - Väljasttellitud tarkvara jälgmine ja kontrollimine - ISO 17799; **Seire ja ülevaade kolmanda osapoolte teenustele/ raportitele** - Teenuseid ja raporteid tuleb regulaarselt jälgida ja üle vaadata - ISO 17799; **Halb väljasttellimise strateegia** - ISKE; **Väljasttellimine** - Väliste tarnijate poolt tehtud süsteemid peavad vastama turvanõuetele - ISF
  Nõrkus: Väljasttellitud tarkvara ei vasta vajalikele tingimustele
  Oht: Toimub rakenduse käideldavuse/tervikluse/konfidentsiaalsuse kadu

- **Kolmandate osapoolte ligipääsetavus** - välised ühendused partnerite ja klientitega peavad olema identifitseeritud ja aktsepteeritud - ISF; **Välised ühendused** - kõik välised ühendused rakendusega peaksid olema määratletud, kontrollitud ja kinnitatud teenuse omaniku poolt - ISF
  Nõrkus: Välised ühenduse partnerite ja klientidega ei ole identifitseeritud/aktsepteeritud
  Oht: Toimub rakenduse käideldavuse/tervikluse/konfidentsiaalsuse kadu

- **Alternatiivne töökorraldus** - alternatiivse töökorralduse plaani olemasolu, testimine ja vajadusel rakendamine - ISF
  Nõrkus: Alternatiivse töökorralduse plaani puudumine

Oht: Olemasolevate vahendite/ressursside puudumisel või tõrkel seiskub töö

5.3. IT ja süsteemid

IT ja süsteemide riskid on seotud eelkõige IT-tehnikaga, seadmetega ja erinevate süsteemidega.

- **Andmebaasi turvamehhanismide puudumine või puudulikkus** (paroolid jms) - ISKE; **Andmebaasisüsteemi hooletu haldus** (liigsed õigused, seire puudumine, harv varukopeerimine) - ISKE
  Nõrkus: Andmebaasi turvamehhanismide puudumine või puudulikkus
  Oht: Ründed andmebaasi pihta, käideldavuse/tervikluse/konfidentsiaalsuse kadu

- **Andmebaasi väljalangemine** (riistvara tõrke, ründe vm tõttu) - ISKE
  Nõrkus: Andmebaasi ebakindlus (riistvara, tarkvara, ründe vms tõttu)
  Oht: Andmebaasi väljalangemine süsteemist

- **Andmete kadu andmebaasis** (kogemata, rünne, rike,...) - ISKE; **Andmete kadu andmebaasis, salvestusruumi puudumise tõttu** - ISKE
  Nõrkus: Andmebaasi administraatori hooletus/teadmatus
  Oht: Andmete(tervikluse) kadu andmebaasist (näiteks salvestusruumi puudumise tõttu)

- **Sisevõrkude katkestus** - ISKE; **Liini piisamatu ribalaius** (võrgu plaanimine tulevikuvaruta) - ISKE; **Võrgu disain** - võrk peab hakkama saama praeguse ja tulevase ennustatava liikluse ja andmemahtudega - ISF; **Võrgu- või süsteemihaldussüsteemi komponendi tõrge** - ISKE
  Nõrkus: Sisevõrkude väike läbilaskevõime
  Nõrkus: Ebakindel võrgukomponent
  Oht: Sisevõrgu katkestus

- **Võrgu seire** - võrgu aktiivsust peab monitoorima - ISF; **Seire** - süsteemi seire ISO 17799; **Sisemiste protsesside kontroll** - sisemiste protsesside jälgimine, et avastada töötlemise käigus tekkinud rikutud informatsiooni - ISO 17799
  Nõrkus: Süsteemide seire puudub või on puudulik
  Oht: Puudub jooksev ülevaade süsteemi tööst ja töökorras olemisest - rikete avastamine võtab liiga palju aega

- **Võrkude eraldamine** - erinevate teenuste võrkude eraldamine - ISO 17799
  Nõrkus: Toodangu, testi ja arenduse keskkonnad on eraldamata
  Oht: Süsteemi käideldavuse/tervikluse kadu

- **Välise teenusetarnija süsteemide tõrge** - ISKE; **Sõltuvus välisest teenusetarnijast** - ISKE
  Nõrkus: Sõltuvus välisest teenusetarnijast
  Oht: Välise teenusetarnija süsteemide tõrge põhjustab nendest sõltuvate siseste teenuste tõrke

- **Elektritoide** - kriitilised teenused peavad olema kaitstud elektrivoolu katkestuste vastu - ISF
  Nõrkus: Kaitsetus elektrivoolu katkemise vastu
  Oht: Süsteemi käideldavuse/tervikluse kadu elektrivoolu katkestuse tagajärjel

- **Installeerimine** - uute süsteemide installeerimine peab käima kooskõlas dokumenteeritud installeerimise protsessiga - ISF
  Nõrkus: Installeerimise protsess dokumenteerimata ja/või seda ei järgita
  Oht: Installeeritakse valesti, valel ajal, valesse kohta, vms

- **Tagavarakoopiad** - Tagavarakoopiate tegemine informatsioonist ja tarkvarast ning nende testimine - ISO 17799; **Varundus** - tagavarakoopiate tegemine regulaarselt olulisest informatsioonist ja tarkvarast, mida rakendus kasutab - ISF

Nõrkus: Puudub regulaarne ja nõuetepärane varundus
Oht: Toimub andmekadu süsteemis

- **Logimine ja logide kaitsemine** - kasutajate ja süsteemi tegevuse logimine - ISO 17799; **Süsteemi administraatori ja operaatori logimine** - süsteemi administraatori tegevuse logimine - ISO 17799; **Vigade logimine** - süsteemis esinevate vigade logimine - ISO 17799; **Sündmuste logimine** - ISF
  Nõrkus: Puudub piisav kasutajate tegevuse logimine
  Oht: Puudub ülevaade, milliseid toiminguid ja transaktsioone kasutajad süsteemis teevad.
  Nõrkus: Puudub piisav süsteemi tegevuste ja vigade logimine
  Oht: Süsteemi maasolekul pole teada, mis viga seda täpsemalt põhjustab

- **Privileegide haldus** - rakenduses privileegide (eriõiguste) kasutamine peab olema piiratud ja kontrollitud - ISO 17799
  Nõrkus: Puudub kontroll eriõiguste üle
  Oht: Kasutajatel õigus toimingutele, mida neil (enam) olla ei tohiks

- **Sisendandmete kontroll** - andmete kontroll enne andmete töötlust - ISO 17799;
  Nõrkus: Puudub sisendandmete kontroll enne andmete töötlust
  Oht: Vigaste sisendandmete tagajärjel tekkinud tervikluse kadu või süsteemi töö häired

- **Väljundandmete kontroll** - väljundandmete kontrollimine, et töödeldud ja salvestatud andmed oleksid õiged - ISO 17799
  Nõrkus: Puudub väljundandmete kontroll peale töötlust
  Oht: Andmetöötluse käigus tekivad vigased andmed

- **Süsteemi vigane arhitektuur** - süsteemi aeglus, vead
  Nõrkus: Süsteemil vigane või puudulik arhitektuur
  Oht: Süsteem ebastabiilne, ettearvamatu, aeglane, raskesti hallatav, ...

- **Elastsus** - Rakendus võiks töötada töökindlal ja usaldusväärsel riistvaral ja tarkvaral, mis on duubeldatud - ISF

  Nõrkus: Rakenduse alusvara ei ole töökindel/usaldusväärne

  Oht: Rakendus võib muutuda ebastabiilseks

  Nõrkus: Rakenduse alusvara ei ole duubeldatud

  Oht: Alusvara tõrke korral võib toimuda rakenduse seisak

  Nõrkus: Rakenduse alusvara jagatakse teiste rakendustega

  Oht: Antud rakenduse seisak põhjustatud teise rakenduse poolt

  Nõrkus: Rakenduse ümberlülitus tagavarasüsteemile ei ole automaatne

  Oht: Ümberlülitus ei toimu ning toimub teenuse seisak

  Nõrkus: Teenus sõltub teistest vähemkriitilistest teenustest

  Oht: Alusvara kriitilisus on väiksem (lubatud rohkem seisakuid), kui sellel toimival teenusel

6. Riskide hindamise mudeli rakenduspõhimõtted

Koostatud mudel nõrkustest peaks olema abiks teenusehalduritele IT missioonikriitiliste teenuste riskide määratlemiseks ja hindamiseks.

Mudel koosneb nõrkustest, mis on jaotatud kolme kategooriasse: personal, protsessid ning IT ja süsteemid.

Teenusehaldur peaks esimesena hindama seda, kui suur on tõenäosus, et mingi oht kasutab ära mõnda mudelis olevat nõrkust. Ehk teisisõnu - kui suur on tõenäosus, et mõni oht või ohud realiseeruvad läbi mudelis olevate nõrkuste.

Hinnang peaks puudutama võimalikku ohu esinemise tõenäosust tulevikus, tuginedes vajadusel ka minevikus toimunud intsidentidele.

Esinemiste tõenäoste astmed võiksid autori arvates olla järgnevad:

1. **Väga madal** - esinemine harvem kui kord 10 aasta jooksul
2. **Madal** - esinemine kord 10 aasta jooksul
3. **Keskmine** - esinemine kord 3 aasta jooksul
4. **Kõrge** - esinemine rohkem kui kord 1 aasta jooksul
5. **Väga kõrge** - esinemine võimalik juba täna

Teisena tuleks hinnata iga nõrkuse puhul ohu võimalikku mõju teenusele. Teenusehalduri jaoks väljendub mõju eelkõige teenuse seisaku pikkuses ja ulatuses - kas mõjutatud on teenuse üksikud ja vähem tähtsad osad või on terve teenus pikalt kättesaamatu.

Mõju suurused võiksid autori arvates olla järgnevad:

1. **Väga madal** - teenuse seisakut ei toimu
2. **Madal** - mõjutatud vähem tähtsad osad, kriitiline funktsionaalsus tagatud
3. **Keskmine** - teenuse lühiaegne seisak
4. **Kõrge** - teenuse seisak pikem, kogu teenus halvatud
5. **Väga kõrge** - teenuse seisak väga pikk, kogu teenus halvatud ja taastamine aeganõudev

Vastavalt konkreetsele ettevõttele tuleks määrata täpsemalt mõisted „lühiaegne“, „pikk“ ja „väga pikk“.

Kolmandana tuleks iga konkreetse nõrkuse puhul hinnata riski suurust. Selle tegemiseks pakub autor välja tabeli(*Tabel 1*), mille põhjal saab leida vastavalt mõjule ja tõenäosusele riski suuruse kolmepallilisel skaalal.

Kus:

V on väike risk

K on keskmine risk

S on suur risk

Mõju

Tõenäosus	**1**	**2**	**3**	**4**	**5**
1	V	V	V	K	K
2	V	V	K	K	S
3	V	K	K	S	S
4	K	K	S	S	S
5	K	S	S	S	S

Tabel 1: Riski suurus

Riski allikate kategooriatest ja prioriteedidest ülevaate saamiseks on abiks järgnev tabel *(Tabel 2)*, kuhu tuleks märkida erinevates riskide kategooriates esinenud riskide arv vastavalt nende suurustele:

	Väike risk (V)	Keskmine risk (K)	Suur risk (S)
Personal			
Protsessid			
IT ja süsteemid			

Tabel 2: Riskide ülevaade

Käesoleva magistritöö Lisast 1 leiab valminud mudeli täidetud näidise.

6.1. Personal

Personaliga seotud ohtude hindamine vastavalt nõrkustele *(Tabel 3)*.

Nõrkus	**Tõenäosus**	**Mõju**	**Riski suurus**
Kompetentse personali vähene töövalmidus/dubleerimatus			
Operatsioonid sisaldavad suurel hulgal käsitsitegevusi			
Ebakompetentne personal (konfigureerimine, IT-süsteemi haldus)			
Personali teadmatus või lohakus andmetega ümber käimisel			
Sõltumine (välistest) konsultantidest			
Kasutajaid ei tööta süsteemidega õigesti			
Turvaintsidentidest raporteerimine puudub või on puudulik			
Turvanõrkusetele ei pöörata tähelepanu			

Tabel 3: Personali nõrkused

6.2. Protsessid

Protsessidega seotud ohtude hindamine vastavalt nõrkustele *(Tabel 4)*.

Nõrkus	**Tõenäosus**	**Mõju**	**Riski suurus**
Informatsioonil või süsteemil puudub omanik			
Töötajate rollid ja vastutused pole täpselt määratletud			
Arenduse poolsete kontaktide ja vastutajate puudumine			
Ebapiisav ligipääs töö tegemiseks			
Liigne pääs töö tegemiseks			
Tarkvara testimine viiakse läbi puudulikult			
Tarkvara testimine viiakse läbi toodangu keskkonnast erinevas keskkonnas			
Süsteemi ja/või operatsioonide kohta puudub korralik dokumentatsioon			
Muudatuste tegemine süsteemides ei ole kontrollitud			
Nõuded uutele süsteemidele ebaselged, defineerimata			
Intsidentide haldus puudub või on puudulik			
Taasteplaan puudub, on puudulik või testimata			
Teenuste taseme lepingud puuduvad			
Väljasttellitud tarkvara ei vasta vajalikele tingimustele			

Nõrkus	**Tõenäosus**	**Mõju**	**Riski suurus**
Välised ühenduse partnerite ja klientidega ei ole identifitseeritud/aktsepteeritud			
Alternatiivse töökorralduse plaani puudumine			

Tabel 4: Protsesside riskid

6.3. IT ja süsteemid

IT ja süsteemidega seotud ohtude hindamine vastavalt nõrkustele *(Tabel 5)*.

Nõrkus	**Tõenäosus**	**Mõju**	**Riski suurus**
Andmebaasi turvamehhanismide puudumine või puudulikkus			
Andmebaasi ebakindlus (riistvara, tarkvara, ründe vms tõttu)			
Andmebaasi administraatori hooletus/teadmatus			
Sisevõrkude väike läbilaskevõime			
Ebakindel võrgukomponent			
Süsteemide seire puudub või on puudulik			
Toodangu, testi ja arenduse keskkonnad on eraldamata			
Sõltuvus välisest teenusetarnijast			
Kaitsetus elektrivoolu katkemise vastu			
Installeerimise protsess dokumenteerimata ja/või seda ei järgita			
Puudub regulaarne ja nõuetepärane varundus			
Puudub piisav kasutajate tegevuse logimine			
Puudub piisav süsteemi tegevuste ja vigade logimine			
Puudub kontroll eriõiguste üle			
Puudub sisendandmete kontroll enne andmete töötlust			

Nõrkus	**Tõenäosus**	**Mõju**	**Riski suurus**
Puudub väljundandmete kontroll peale töötlust			
Süsteemil vigane või puudulik arhitektuur			
Rakenduse alusvara ei ole töökindel/usaldusväärne			
Rakenduse alusvara ei ole duubeldatud			
Rakenduse alusvara jagatakse teiste rakendustega			
Rakenduse ümberlülitus tagavarasüsteemile ei ole automaatne			
Teenus sõltub teistest vähemkriitilistest teenustest			

Tabel 5: IT ja süsteemide riskid

7. Kokkuvõte

Käesoleva magistritöö eesmärgiks oli leida või koostada sobiv mudel IT missioonikriitiliste teenuste riskide määratlemiseks ja hindamiseks ning seda eelkõige teenusehalduritele.

Magistritöö raames uuriti erinevaid turvastandardeid, etalonturbe süsteeme ja nendega seonduvaid materjale.

Kuna sobivat valmis olevat mudelit ei leitud, siis sai autori poolt uuritavate materjalide põhjal koostatud ise vajalik mudel. Selleks koguti uuritavatest materjalidest kokku erinevad teenusehaldurit puudutavad punktid, jagati need parema ülevaate saamiseks kolme suuremasse kategooriasse(personal, protsessid, IT ja süsteemid) ning määrati neile vastavad nõrkused ja pakuti välja ka võimalikud täpsustavad ohud.

Antud mudeli puhul on teenusehalduri ülesandeks määrata erinevate nõrkuste puhul tõenäosused, et mõni oht võib seda ära kasutada ja hinnata võimaliku tagajärje mõju. Vastavalt tõenäosusele ja mõjule määratakse riski suurus, mille puhul on hea saada ülevaadet riskide olulisusest ja teha plaane vastavalt nende prioriteetidele.

Magistritöö tulemusena valmis lihtsasti kasutatav mudel teenusehalduritele IT missioonikriitiliste teenuste riskide hindamiseks.

Antud mudel vajaks ilmselt peale põhjalikumat kasutamist ülevaatamist ja parendamist, kuid Hansapanga IT-riskijuhid on öelnud, et loodud mudel on ka praegusel hetkel kindlasti praktikas kasutatav IT halduses töötavatele spetsialistidele, kelle põhitöö ei ole riskijuhtimine, kuid kes peavad arvestama oma töös negatiivsete stsenaariumitega. Loodud mudel pakub põhiküsimustikku, mille abil saab IT halduse töötaja määratleda olulisemaid riske, mille maandamisega tuleb esmajärjekorras tegeleda.

8. Summary

The purpose of the current Master`s thesis was to find or put together a suitable model to define and assess the risks of mission critical IT services, mostly for service managers.

In the course of the master`s thesis different security standards, etalon security systems and associated materials were studied.

Since a suitable and complete model was not found, then the appropriate model was constructed according to the materials studied by the autor. For that purpose different service manager related points were gathered from the studied materials, divided into three bigger cathegories (personnel, processes, IT and systems) for a better overview and corresponding weaknesses were assigned and also possible adjustable dangers were presented.

In case of the current model the duty of the service manager is to assign probabilities to different weaknesses that some threat could take advantage of those weaknesses. Another assignment is assessing possible impact of the consequences. The risk dimensions are determined on the basis of the probability and impact of the possible threats thus creating a good overview of the risks` importance and possibility to create plans according to those priorities.

As a result of the master`s thesis an easily usable mission-critical IT service risk assessment model was made.

Naturally this model would need overview and improvement after practicing, but experts have rated the model as sufficiently usable model as it is.

9. Kasutatud kirjandus

- [1] Infosüsteemide turve 1 - Turvarisk - Küberneetika AS, 1997
- [2] Infosüsteemide kolmeastmelise etalonturbe süsteem - ISKE rakendusjuhend versioon 3, september 2007
- [3] ISO/IEC 17799:2005(E) Information technology - Security techniques - Code of practice for information security management
- [4] ISO 13335-1:2004 Information technology - Security techniques - Management of information and communications technology security
- [5] The Standard of Good Practice for Information Security, 2007.a. - Information Security Forum (ISF)
- [6] IT Infrastructure Library (ITIL), Service Operation, TSO (The Stationery Office), 2007
- [7] IT Infrastructure Library (ITIL), Service Support, Best Practice, CD-rom version, 2000
- [8] IT Service Management Forum, ITSM Library - Foundations of IT Service Management Based on ITIL V3, 2007

10. Lisa 1

Antud lisas on välja toodud valminud mudel täidetud näidis.

Personaliga seotud ohtude hindamine vastavalt nõrkustele *(Tabel 6)*.

Nõrkus	**Tõenäosus**	**Mõju**	**Riski suurus**
Kompetentse personali vähene töövalmidus/dubleerimatus	3	3	K
Personali teadmatus või lohakus andmetega ümber käimisel	3	4	S
Operatsioonid sisaldavad suurel hulgal käsitsitegevusi	5	4	S
Ebakompetentne personal (konfigureerimine, IT-süsteemi haldus)	4	4	S
Sõltumine (välistest) konsultantidest	1	2	V
Kasutajaid ei tööta süsteemidega õigesti	1	1	V
Turvaintsidentidest raporteerimine puudub või on puudulik	1	1	V
Turvanõrkusetele ei pöörata tähelepanu	2	4	K

Tabel 6: Personali nõrkused

Protsessidega seotud ohtude hindamine vastavalt nõrkustele *(Tabel 7)*.

Nõrkus	**Tõenäosus**	**Mõju**	**Riski suurus**
Informatsioonil või süsteemil puudub omanik	2	1	V
Töötajate rollid ja vastutused pole täpselt määratletud	3	4	S
Arenduse poolsete kontaktide ja vastutajate puudumine	3	4	S
Ebapiisav ligipääs töö tegemiseks	2	3	K
Liigne pääs töö tegemiseks	1	1	V
Tarkvara testimine viiakse läbi puudulikult	4	5	S
Tarkvara testimine viiakse läbi toodangu keskkonnast erinevas keskkonnas	4	4	S
Süsteemi ja/või operatsioonide kohta puudub korralik dokumentatsioon	2	1	V
Muudatuste tegemine süsteemides ei ole kontrollitud	2	2	V
Nõuded uutele süsteemidele ebaselged, defineerimata	1	1	V
Intsidentide haldus puudub või on puudulik	1	1	V
Taasteplaan puudub, on puudulik või testimata	1	5	K
Teenuste taseme lepingud puuduvad	1	1	V
Väljasttellitud tarkvara ei vasta vajalikele tingimustele	1	1	V
Välised ühenduse partnerite ja klientidega ei ole identifitseeritud/aktsepteeritud	1	1	V
Alternatiivse töökorralduse plaani puudumine	1	5	K

Tabel 7: Protsesside riskid

IT ja süsteemidega seotud ohtude hindamine vastavalt nõrkustele *(Tabel 8)*.

Nõrkus	**Tõenäosus**	**Mõju**	**Riski suurus**
Andmebaasi turvamehhanismide puudumine või puudulikkus	1	1	V
Andmebaasi ebakindlus (riistvara, tarkvara, ründe vms tõttu)	2	5	S
Andmebaasi administraatori hooletus/teadmatus	1	4	K
Sisevõrkude väike läbilaskevõime	1	2	V
Ebakindel võrgukomponent	2	3	K
Süsteemide seire puudub või on puudulik	1	2	V
Toodangu, testi ja arenduse keskkonnad on eraldamata	1	1	V
Sõltuvus välisest teenusetarnijast	1	1	V
Kaitsetus elektrivoolu katkemise vastu	2	5	S
Installeerimise protsess dokumenteerimata ja/või seda ei järgita	1	1	V
Puudub regulaarne ja nõuetepärane varundus	1	5	K
Puudub piisav kasutajate tegevuse logimine	1	1	V
Puudub piisav süsteemi tegevuste ja vigade logimine	2	3	K
Puudub kontroll eriõiguste üle	1	2	V
Puudub sisendandmete kontroll enne andmete töötlust	2	4	K
Puudub väljundandmete kontroll peale töötlust	1	1	V
Süsteemil vigane või puudulik arhitektuur	1	1	V

Nõrkus	**Tõenäosus**	**Mõju**	**Riski suurus**
Rakenduse alusvara ei ole töökindel/usaldusväärne	4	5	S
Rakenduse alusvara ei ole duubeldatud	3	4	S
Rakenduse alusvara jagatakse teiste rakendustega	1	1	V
Rakenduse ümberlülitus tagavarasüsteemile ei ole automaatne	3	3	K
Teenus sõltub teistest vähemkriitilistest teenustest	3	3	K

Tabel 8: IT ja süsteemide riskid

Ülevaade riski allikatest*(Tabel 9)*:

	Väike risk (V)	Keskmine risk (K)	Suur risk (S)
Personal	3	2	3
Protsessid	9	3	4
IT ja süsteemid	11	7	4

Tabel 9: Ülevaade riskidest