PROUD ENGINEERS

Keskne volituste, rollide ja pääsuõiguste haldamise süsteem

Riskianalüüs

Koostaja: Proud Engineers OÜ

Versioon: 1.1

Kuupäev: 28.12.2021

Proud Engineers OÜ | Kristjani tee 4, 74015 Miiduranna, Estonia
getstarted@proudengineers.ee | proudengineers.ee

Sisukord

1. Sissejuhatus

Käesoleva dokumendi eesmärk on anda ülevaade kõrge taseme riskidest seoses keskse pääsuhalduse lahenduse käitamisega. Eeldatakse, et lahendus on loodud vastavalt esitatud arhitektuuridokumendile[1]. Kuna infosüsteemi riskid oma olemuselt on tugevas sõltuvuses infosüsteemi realisatsioonist ja paigaldusest ning neid mõlemat ümbritsevatest protsessidest on käesolev dokument mõeldud eelkõige sisendina edasisele riskihaldusprotsessile ning annab üldise ülevaate keskse pääsuhalduse lahenduse loomisega seotud riskidest.

Dokumendi koostamisel tugineti Eesti infoturbestandardi (E-ITS) Riskihaldusjuhendile[2] viies läbi riski kaalutlemise sammu, mis koosneb riskide tuvastamisest, analüüsist ja hindamisest. Dokumendis on kasutusel samas määratletud riskihalduse astmestikke ning muud terminoloogiat.

Täpsemalt viidi läbi järgmised tegevused:

- Riskituvastus
    - Vastavalt kolmele infoturbe komponendile (konfidentsiaalsus, terviklus ja käideldavus) loetleti peamised potentsiaalsed kahjud
    - Iga leitud kahju jaoks koostati riskipuu, mis seob riskid konkreetsete kahjudega
- Riskianalüüs
    - Leitud riskid seoti alusohtudega
    - Leitud riskid hinnati kas lahenduse skoobis olevateks (st. nende maandamine on lahendust arendava ja käitava organisatsiooni vastutus) või sellest väljapoole jäävateks (st. nende maandamine on kellegi teise vastutus)
    - Eemaldati dubleerivad riskid sidudes riskipuud omavahel ja liites sama mõjuga riske
- Riski hindamine
    - Riskidele omistati ohu realiseerumise sageduse ja potentsiaalse kahju hinnangud

Riskide hindamisel kasutati järgmisi astmikke[3]:

---

[1] Vt "Tulevikulahenduse arhitektuur".
[2] Eesti infoturbe standardi portaal, https://eits.ria.ee/et/versioon/2020vers1/standardi-dokumendid/riskihaldusjuhend.
[3] E-ITS Riskihaldusjuhend 4.3.1.1 ja 4.3.1.2

- Potentsiaalne kahju
    - **Ähvardab organisatsiooni olemasolu.** Kahjud võivad ulatuda katastroofilise tasemeni, mis ähvardab organisatsiooni olemasolu
    - **Tõsine**. Kahjud võivad olla tõsised
    - **Piiratud**. Kahjud on piiratud ja nendega saab hakkama
    - **Tühine**. Kahjud on väikesed ja nendega saab jätta arvestamata
- Realiseerumise võimalikkus
    - **Väga sage**. Sündmus toimub mitu korda kuus
    - **Sage**. Sündmus toimub kord kuus kuni kord aastas
    - **Keskmine**. Sündmus toimub üks kord iga ühe kuni viie aasta kohta
    - **Harv**. Senise teadmuse põhjal võib sündmus toimuda maksimaalselt üks kord viie aasta jooksul

Riskianalüüsi skoobis on ainult keskne pääsuhalduse lahendus. Seega on analüüsi skoobist on väljas kõik riskid, mida keskne pääsuhalduse lahendus võib põhjustada teistele, liidestatud, süsteemidele. Näiteks ei käsitleta rahvastiku- või äriregistri pihta suunatud andmete korrutamise ründeid, milleks võib võimaluse anda otsingu liides või teenustõrke ründeid, mida võib realiseerida allikregistrite suunas kas tahtlikult või tahtmatult saadetud liiga suur päringute hulk. Samuti ei käsitle analüüs kesksest lahendusest, allikregistritest ja klientsüsteemidest koosnevat pääsuhalduse süsteemi kui tervikut, näiteks on skoobist väljas ründed äriregistri vastu, mille ebakorrektsed vastused kesksele pääsuhalduse lahendusele viivad volitamata ligipääsuni EMTA infosüsteemile.

Läbi viidud kaalutlusprotsessi tulemuseks on riskide nimekiri koos riski suuruse hinnanguga, riskipuud ning kokkuvõttev ülevaade riskidest.

2. Riskianalüüs

Riskituvastuse faasis leiti kolm peamist ohtu:

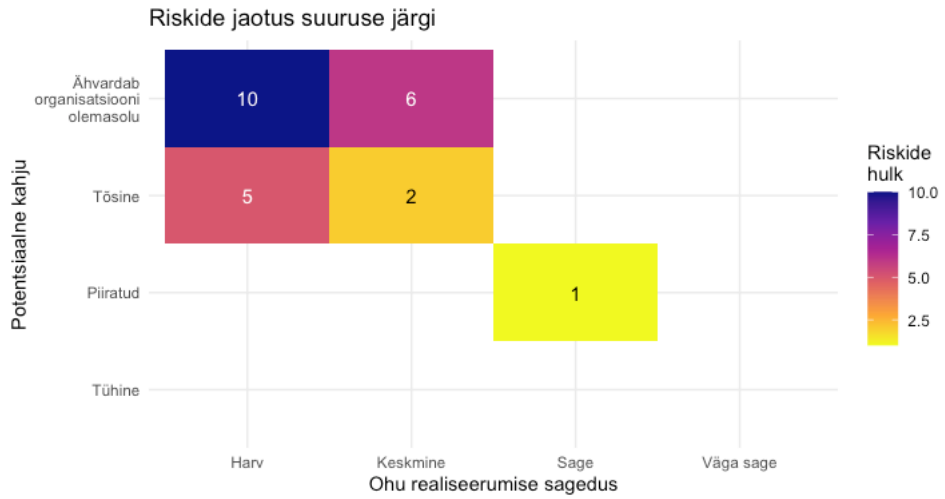
- **Keskne pääsuhalduse lahendus ei suuda väljastada infot rolli olemasolu kohta**. Tegemist on käideldavuse (A) komponendi ohuga. Ohu realiseerumisel on kas osaliselt või täielikult takistatud keskse pääsuhalduse lahenduse võime väljastada teenuslepingus sätestatud piires infot rolli olemasolu kohta.
- **Keskne pääsuhalduse lahendus väljastab ebakorrektse info rolli olemasolu kohta**. Tegemist on tervikluse (I) ohuga. Ohu realiseerumisel juhul väljastab keskne pääsuhalduse lahendus ebakorrektset infot rollide olemasolu kohta. Ebakorrektseks

loetakse vastust, mis ei ühti kasutaja väljendatud tahtega või ei kajasta korrektselt allikregistrites asuvat infot rollide kohta.

- **Keskse pääsuhalduse lahenduse andmed saavad avalikuks**. Tegemist on konfidentsiaalsuse (C) ohuga. Ohu realiseerumisel saavad kas kasutaja poolt määratud või allikregistritest päritud rollimäärangud (sh. näiteks perekondlikud ja ärilised suhted) või ka isikute nimed kättesaadavaks selleks volitamata isikutele.

Enamik leitud riske klassifitseerub suuruse alusel keskmiseks, kuid leidub ka suuri riske. Oluline on, et suur hulk riske on oma olemuselt eksistentsiaalse mõjuga, sest keskse pääsuhalduse lahenduse süstemaatiliselt valed vastused võimaldavad lubamatut ligipääsu kõigile seda kasutavatele infosüsteemidele ning tema tõrge tähendab kõigi temaga täisintegratsiooni[4] realiseerinud infosüsteemide tõrget. Riskide jaotuse võtab kokku Joonis 1.

Ohtude kaupa grupeeritud riske sisaldavad Tabel 1, Tabel 2 ja Tabel 3.



Joonis 1. Riskide jaotus suuruse järgi

[4] Mudel, kus infosüsteem loobub täielikult oma pääsuhalduse lahendusest ja kasutab selleks keskset lahendust.

Tabel 1. Keskne pääsuhalduse lahendus ei suuda väljastada infot rolli olemasolu kohta (A)

Risk	**Alusoht**	**Skoobis**	**Potentsiaalne kahju**	**Ohu realiseerumise võimalikkus**	**Riski suurus**
R9. Toimub edukas rünne keskse pääsuhalduse lahenduse alusinfrastruktuuri vastu	G0.14, G0.16, G0.17, G0.19, G0.21, G0.23, G0.28, G0.29, G0.30, G0.34, G0.36, G0.39, G0.41, G0.45	EI	Ähvardab organisatsiooni olemasolu	Keskmine	Suur
R16. Andmete riknemine viib ebakorrektse info väljastamiseni keskse pääsuhalduse lahenduse poolt	G0.9, G0.18, G0.20, G0.25, G0.26, G0.28, G0.46	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine
R18. Keskse pääsuhalduse lahenduse rollide konfiguratsioon muutub kas süntaktiliselt või sisuliselt ebakorrektseks	G0.9,G0.18, G0.26, G0.28, G0.29, G0.31, G0.46	JAH	Tõsine	Harv	Keskmine

Risk	Alusoht	Skoobis	Potentsiaalne kahju	Ohu realiseerumise võimalikkus	Riski suurus
R19. Keskse pääsuhalduse lahenduse infrastruktuur tõrgub	G0.1, G0.2, G0.3, G0.4, G0.5, G0.6, G0.8, G0.9, G0.10, G0.12, G0.20, G0.25, G0.27, G0.29, G0.34, G0.39, G0.40, G0.41, G0.44, G0.45	EI	Ähvardab organisatsiooni olemasolu	Keskmine	Suur
R20. Toimub edukas teenustõrke rünne keskse pääsuhalduse lahenduse vastu	G0.40	JAH	Tõsine	Harv	Keskmine
R21. Keskse pääsuhalduse lahenduse koodi riknemine põhjustab teenuse tõrke	G0.18, G0.20, G0.28, G0.29, G0.33, G0.45, G0.47	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine

Tabel 2. Keskne pääsuhalduse lahendus väljastab ebakorrektse info rolli olemasolu kohta (I)

Risk	**Alusoht**	**Skoobis**	**Potentsiaalne kahju**	**Ohu realiseerumise võimalikkus**	**Riski suurus**
R1. Volitatud juurdepääsuga isik muudab tahtlikult rakenduse lähtekoodi põhjustades ebakorrektse vastuse	G0.14, G0.29, G0.31, G0.32, G0.35, G0.42	JAH	Ähvardab organisatsiooni olemasolu	Keskmine	Suur
R2. Volitamata juurdepääsuga isik muudab tahtlikult rakenduse lähtekoodi põhjustades ebakorrektse vastuse	G0.14, G0.16, G0.17, G0.19, G0.21, G0.23, G0.28, G0.29, G0.30, G0.34, G0.36, G0.39, G0.41, G0.44, G0.46	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine
R3. Volitamata juurdepääsuga isik saab juurdepääsu keskse pääsuhalduse	G0.14, G0.16, G0.17, G0.19, G0.21, G0.23,	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine

Risk	Alusoht	Skoobis	Potentsiaalne kahju	Ohu realiseerumise võimalikkus	Riski suurus
lahenduse infrastruktuurile	G0.28, G0.29, G0.30, G0.34, G0.36, G0.39, G0.41, G0.44				
R4. Volitatud juurdepääsuga isik väärkasutab keskse pääsuhalduse lahenduse infrastruktuuri	G0.14, G0.29, G0.31, G0.32, G0.35, G0.42,	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine
R5. Toimub edukas rünne lõppkasutaja identiteedi vastu	G0.36	EI	Piiratud	Sage	Keskmine
R6. Haavatavus keskse pääsuhalduse lahenduse koodis võimaldab muuta antud volitusi	G0.28	JAH	Tõsine	Keskmine	Keskmine
R7. Volitamata juurdepääsuga isik muudab	G0.14, G0.16, G0.17,	JAH	Ähvardab organisatsiooni olemasolu	Keskmine	Suur

Risk	Alusoht	Skoobis	Potentsiaalne kahju	Ohu realiseerumise võimalikkus	Riski suurus
keskse pääsuhalduse lahenduse rollide konfiguratsiooni	G0.19, G0.21, G0.23, G0.28, G0.29, G0.30, G0.34, G0.36, G0.39, G0.41, G0.44				
R8. Volitatud juurdepääsuga isik muudab lubamatult keskse pääsuhalduse lahenduse rollide konfiguratsiooni	G0.14, G0.29, G0.31, G0.32, G0.35, G0.42,	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine
R11. Toimub edukas rünne allikregistri või X-tee taristu vastu	G0.14, G0.16, G0.17, G0.19, G0.21, G0.23, G0.28, G0.29, G0.30, G0.34, G0.36,	EI	Ähvardab organisatsiooni olemasolu	Keskmine	Suur

Risk	Alusoht	Skoobis	Potentsiaalne kahju	Ohu realiseerumise võimalikkus	Riski suurus
	G0.39, G0.41, G0.44				
R12. Keskne pääsuhalduse lahendus interpreteerib valesti kas allikregistrist või kasutajalt saadud infot rollide kohta	G0.20, G0.26, G0.28	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine
R13. Keskne pääsuhalduse lahendus realiseerib ebakorrektselt arvutatud rollide aritmeetika	G0.20, G0.26, G0.28	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine
R14. Keskne pääsuhalduse lahendus reageerib valesti ebakorrektsele sisemisele olekule	G0.20, G0.26, G0.28	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine

Risk	Alusoht	Skoobis	Potentsiaalne kahju	Ohu realiseerumise võimalikkus	Riski suurus
R16. Andmete riknemine viib ebakorrektse info väljastamiseni keskse pääsuhalduse lahenduse poolt	G0.9, G0.18, G0.20, G0.25, G0.26, G0.28, G0.45	JAH	Ähvardab organisatsiooni olemasolu	Harv	Keskmine
R18. Keskse pääsuhalduse lahenduse rollide konfiguratsioon muutub kas süntaktiliselt või sisuliselt ebakorrektseks	G0.9,G0.18, G0.26, G0.28, G0.29, G0.31, G0.45	JAH	Tõsine	Harv	Keskmine

Tabel 3. Keskse pääsuhalduse lahenduse andmed saavad avalikuks (C)

Risk	**Alusoht**	**Skoobis**	**Potentsiaalne kahju**	**Ohu realiseerumise võimalikkus**	**Riski suurus**
R3. Volitamata juurdepääsuga isik saab juurdepääsu keskse pääsuhalduse lahenduse infrastruktuurile	G0.14, G0.16, G0.17, G0.19, G0.21, G0.23, G0.28, G0.29, G0.30, G0.34, G0.36, G0.39, G0.41, G0.44	JAH	Tõsine	Keskmine	Keskmine
R4. Volitatud juurdepääsuga isik väärkasutab keskse pääsuhalduse lahenduse infrastruktuuri	G0.14, G0.29, G0.31, G0.32, G0.35, G0.42,	JAH	Tõsine	Harv	Keskmine
R9. Toimub edukas rünne keskse pääsuhalduse lahenduse alusinfrastruktuuri vastu	G0.14, G0.16, G0.17, G0.19, G0.21, G0.23, G0.28, G0.29, G0.30,	EI	Ähvardab organisatsiooni olemasolu	Keskmine	Suur

Risk	Alusoht	Skoobis	Potentsiaalne kahju	Ohu realiseerumise võimalikkus	Riski suurus
	G0.34, G0.36, G0.39, G0.41, G0.44				
R15. Keskse pääsuhalduse lahenduse konfiguratsioon võimaldab lubamatut ligipääsu töödeldavatele andmetele	G0.26, G0.29, G0.31	JAH	Tõsine	Harv	Keskmine

3. Meetmed

Riskide maandamiseks on võimalik rakendada rida meetmeid. Kuigi teatud meetmeid on võimalik kirjeldada ka süsteemi praeguses, arhitektuuri loomise, faasis, on suur osa meetmeid tugevas sõltuvuses süsteemi operatiivsest keskkonnast. Seetõttu on meetmeid, millede osas on märgitud lihtsalt E-ITS meetmete grupp ja mitte konkreetne tegevus või vahend. Meetmed võtab kokku Tabel 4. Meetmete seosed riskidega on toodud tabelis Tabel 5 ning neist annab ülevaate Joonis 3.

Tabel 4. Riskide maandamiseks rakendatavad meetmed

Meede	Selgitus
M1. INF, OPS ja SYS grupi meetmed	E-ITS etalonturbe kataloogi vastavasse jaotisse kuuluvad meetmed, vastavalt realisatsioonile ja vajadusele

Meede	Selgitus
M2. Konfiguratsiooni halduse protsess	Tugeva kontrolli all, läbi mõeldud ja kõrge küpsusastmega konfiguratsiooni halduse protsess (sh. seoste detailne kirjeldamine)[5]
M3. ORP grupi meetmed	E-ITS etalonturbe kataloogi vastavasse jaotisse kuuluvad meetmed, vastavalt realisatsioonile ja vajadusele
M4. Testimine	Tarkvara automaat- ja manuaaltestimine, laiemalt tarkvara kvaliteediprotsessid
M5. Kinnine koodirepositoorium	Piiratud juurepääsuga koodihoidla kasutamine arenduseks ja tarneks
M6. Pidev (logide) monitooring	Protsess, mis pidevalt jälgib süsteemi tervist ning suudab reageerida kõrvalekalletele normist[6]
M7. *Code-review* protsess (nelja silma printsiip)	Koodi ülevaatuse protsess, mis teeb võimatuks üksiku arendaja muutuste jõudmise tarneahelasse ning tagab, et iga muutust on üle vaadanud vähemalt kaks arendajat, kelledest üks ei ole muutuse autor
M8. Taustakontroll	Süsteemi suhtes ligipääsu omavate isikute suhtes rakendatav taustakontroll
M9. Stabiilne ja lihtne tarneprotsess	Kõrge küpsusastmega, hästi läbi mõeldud ja seejuures kõrge automatiseeritusega ning lihtsasti järgitav tarneprotsess, mis kasutab ainult kontrollitud koodi-ja sõltuvuste hoidlaid
M10. Perioodiline staatiline koodianalüüs	Perioodiliselt läbi viidav rakenduse koodi staatiline analüüs, näiteks kasutades LFX vahendeid, mida kasutatakse Linuxi tuuma tarneahelate tervikluse kontrolliks
M11. Atributeeritud muutused	Kõik muudatused koodis on seotavad nii selle autori kui koodi üle vaadanud arendajaga

[5] Vt „Tulevikulahenduse arhitektuur" p 5.2.6.
[6] Vt „Tulevikulahenduse arhitektuur" p 5.2.7.

Meede	Selgitus
M12. Sõltuvuste haldus	Protsess, mis tagab, et süsteem kasutab võimalikult uusi teekide versioone, millele on rakendatud kõik teadaolevad turvapaigad ning ei kasuta teekide versioone, millede osas leidub paikadeta kuid teadaolevaid haavatavusi
M13. Perioodilised penetratsioonitestid	Perioodiliselt läbi viidavad süsteemi penetratsioonitestid

Tabel 5. Riskide ja meetmete seosed

	M1. INF, OPS ja SYS grupi meetmed	**M2. Konfiguratsiooni halduse protsess**	**M3. ORP grupi meetmed**	**M4. Testimine**	**M5. Kinnine koodirepositoorium**	**M6. Pidev (logide) monitooring**	**M7. Code-review protsess (nelja silma printsiip)**	**M8. Taustakontroll**	**M9. Stabiilne ja lihtne tarneprotsess**	**M10. Perioodiline staatiline koodianalüüs**	**M11. Atributeeritud muutused**	**M12. Sõltuvuste haldus**	**M13. Perioodilised penetratsioonitestid**
R1. Volitatud juurdepääsuga isik muudab tahtlikult rakenduse lähtekoodi põhjustades ebakorrektse vastuse							X	X					

	M1. INF, OPS ja SYS grupi meetmed	M2. Konfiguratsiooni halduse protsess	M3. ORP grupi meetmed	M4. Testimine	M5. Kinnine koodirepositoorium	M6. Pidev (logide) monitooring	M7. Code-review protsess (nelja silma printsiip)	M8. Taustakontroll	M9. Stabiilne ja lihtne tarneprotsess	M10. Perioodiline staatiline koodianalüüs	M11. Atributeeritud muutused	M12. Sõltuvuste haldus	M13. Perioodilised penetratsioonitestid
R2. Volitamata juurdepääsuga isik muudab tahtlikult rakenduse lähtekoodi põhjustades ebakorrektse vastuse					X				X	X	X		
R3. Volitamata juurdepääsuga isik saab juurdepääsu keskse pääsuhalduse lahenduse infrastruktuurile	X												
R4. Volitatud juurdepääsuga isik väärkasutab keskse pääsuhalduse lahenduse infrastruktuuri			X					X					

	M1. INF, OPS ja SYS grupi meetmed	M2. Konfiguratsiooni halduse protsess	M3. ORP grupi meetmed	M4. Testimine	M5. Kinnine koodirepositoorium	M6. Pidev (logide) monitooring	M7. Code-review protsess (nelja silma printsiip)	M8. Taustakontroll	M9. Stabiilne ja lihtne tarneprotsess	M10. Perioodiline staatiline koodianalüüs	M11. Atributeeritud muutused	M12. Sõltuvuste haldus	M13. Perioodilised penetratsioonitestid
R6. Haavatavus keskse pääsuhalduse lahenduse koodis võimaldab muuta antud volitusi						X	X			X		X	X
R7. Volitamata juurdepääsuga isik muudab keskse pääsuhalduse lahenduse rollide konfiguratsiooni	X												
R8. Volitatud juurdepääsuga isik muudab lubamatult keskse pääsuhalduse lahenduse			X					X					

	M1. INF, OPS ja SYS grupi meetmed	M2. Konfiguratsiooni halduse protsess	M3. ORP grupi meetmed	M4. Testimine	M5. Kinnine koodirepositoorium	M6. Pidev (logide) monitooring	M7. Code-review protsess (nelja silma printsiip)	M8. Taustakontroll	M9. Stabiilne ja lihtne tarneprotsess	M10. Perioodiline staatiline koodianalüüs	M11. Atributeeritud muutused	M12. Sõltuvuste haldus	M13. Perioodilised penetratsioonitestid
rollide konfiguratsiooni													
R12. Keskne pääsuhalduse lahendus interpreteerib valesti kas allikregistrist või kasutajalt saadud infot rollide kohta		X		X									
R13. Keskne pääsuhalduse lahendus realiseerib ebakorrektselt arvutatud rollide aritmeetika				X		X							
R14. Keskne pääsuhalduse lahendus reageerib valesti				X		X							

	M1. INF, OPS ja SYS grupi meetmed	M2. Konfiguratsiooni halduse protsess	M3. ORP grupi meetmed	M4. Testimine	M5. Kinnine koodirepositoorium	M6. Pidev (logide) monitooring	M7. Code-review protsess (nelja silma printsiip)	M8. Taustakontroll	M9. Stabiilne ja lihtne tarneprotsess	M10. Perioodiline staatiline koodianalüüs	M11. Atributeeritud muutused	M12. Sõltuvuste haldus	M13. Perioodilised penetratsioonitestid
ebakorrektsele sisemisele olekule													
R15. Keskse pääsuhalduse lahenduse konfiguratsioon võimaldab lubamatut ligipääsu töödeldavatele andmetele	X												
R16. Andmete riknemine viib ebakorrektse info väljastamiseni keskse pääsuhalduse lahenduse poolt	X												
R18. Keskse pääsuhalduse lahenduse rollide		X											

	M1. INF, OPS ja SYS grupi meetmed	M2. Konfiguratsiooni halduse protsess	M3. ORP grupi meetmed	M4. Testimine	M5. Kinnine koodirepositoorium	M6. Pidev (logide) monitooring	M7. Code-review protsess (nelja silma printsiip)	M8. Taustakontroll	M9. Stabiilne ja lihtne tarneprotsess	M10. Perioodiline staatiline koodianalüüs	M11. Atributeeritud muutused	M12. Sõltuvuste haldus	M13. Perioodilised penetratsioonitestid
konfiguratsioon muutub kas süntaktiliselt või sisuliselt ebakorrektseks													
R20. Toimub edukas teenustõrke rünne keskse pääsuhalduse lahenduse vastu	X												
R21. Keskse pääsuhalduse lahenduse koodi riknemine põhjustab teenuse tõrke									X		X		

4. Kokkuvõte

Keskse pääsuhalduse lahenduse riskianalüüs leidis kolm peamist ohtu, mis vastavad kolmele infoturbe komponendile: lahendus kas ei toimi vastavalt nõuetele, väljastab ebakorrektset informatsiooni või kaob kontroll lahenduses töödeldavate andmete üle. Kõik ohud seoti E-ITS kataloogi alusohtudega ning leiti riskid, mille realiseerumisel oht tekib.

Enamik leitud riskidest klassifitseerus keskmiseks, enamasti on riskide realiseerumise tõenäosus madal kuid nende potentsiaalne mõju eksistentsiaalse iseloomuga. Siiski leidub ka suuri ohte. Tuvastatud riskide maandamiseks koostati osalt E-ITS kataloogile tuginedes vajalike meetmete nimekiri, enamik meetmeid maandab mitmeid riske. Seejuures saab sõltub suure osa meetmete detailne realisatsioon infosüsteemi ning seda ümbritseva protsessitaristu realisatsioonist ning arhitektuuri faasis on võimalik vaid meetmete grupi määratlemine.

Lisa 1 - Riskipuu

Joonis 2. Riskipuu

Lisa 2 - Riskide ja meetmete seosed

Joonis 3. Riskide ja meetmete seosed