Projekti „Elutähtsate teenuste osutamist mõjutavate tegurite kaardistamise uuring“ kokkuvõte

November 2016

Lühiülevaade

Käesolev dokument on Riigi Infosüsteemi Ameti (RIA) poolt tellitud projekti „Elutähtsate teenuste osutamist mõjutavate tegurite kaardistamise uuring“ kokkuvõte. Uuring viidi läbi Euroopa Liidu struktuuritoetuse toetusskeemist „Infoühiskonna teadlikkuse tõstmine“, mida rahastab Euroopa Regionaalarengu Fond.

Uuringu peamine eesmärk oli tõsta riigi teadlikkust olulistest elutähtsa teenuse toimepidevust mõjutavatest infotehnoloogilistest rist- ja välissõltuvustest ning saada ülevaade olemasolevatest alternatiivlahendustest (nt käsitsijuhtimise võimekus, varutoiteallikad, dubleeritud andmesideteenus), toimepidevusplaanidest ning infotehnoloogiliste riskide realiseerumise ja elutähtsa teenuse osutamise katkemise taastamise võimekuste kohta. Uuringu käigus analüüsiti uuringu valimis olnud 24 elutähtsa teenuse osutaja (ETO) olemasolevaid protsesse ja alternatiivlahendusi, et saada ülevaade teenuste talitluspidevuse tagamisest teenuse võimaliku katkemise korral.

Töö tulemusena koostasime riigi toimimiseks vajalike elutähtsate teenuste kaardistuse, kus tõime välja teenuste olulisemad infotehnoloogilised Eesti sisesed ristsõltuvused ja riigivälised välissõltuvused koos seotud info- ja kommunikatsioonitehnoloogia (IKT) komponentidega. Kaardistasime võimalikud riskid, mis võivad mõjutada Eesti Vabariigis elutähtsate teenuste osutamist. Selgitasime välja asutused, mis suudavad riskide realiseerumisel teenuste osutamist alternatiivlahendustega tagada.

Uuringu raames keskenduti elutähtsa teenuse osutamisega seotud infotehnoloogilistele käitavatele ja toetavatele süsteemidele. Viidi läbi elutähtsa teenuse osutamiseks missioonikriitiliste teenuste, taristu ja muude komponentide analüüs, et tuvastada võimalikud sõltuvused ja ohud tulenevalt väljast tellitud teenusepakkujast nii riigisiseselt kui ka väljaspool Eesti territooriumi.

Uuringu sihtrühm

KPMG lähtus tööde läbiviimisel kehtivas hädaolukorra seaduses (HOS) (vastu võetud 15.06.2009, RT I 2009, 39, 262) esitatud elutähtsa teenuse määratlusest ning kohustustest elutähtsa teenuse talitluspidevuse tagamisel, uuring hõlmas HOS-s sätestatud elutähtsaid teenuseid ja nende osutajaid. Sihtgruppi kuulus 12 elutähtsate teenuste valdkonda ning igast valdkonnast kaasati uuringusse kaks tellija hinnangul olulise mõjuga teenuseosutajat.

Käsitletud elutähtsate teenuste valdkonnad olid:

- elektriga varustamine (tootmine, põhivõrk ja jaotusvõrk);
- maagaasiga varustamine (põhivõrk ja jaotusvõrk);
- vedelkütusega varustamine;
- riigimaanteede ja kohalike teede sõidetavus;
- telekommunikatsiooni teenused (telefon, mobiiltelefon ja andmeside);
- tervishoiuteenus (vältimatu abi);
- finantsteenused (makseteenus, sularaharinglus);
- kaugküttega varustamine;
- veevarustamise ja kanalisatsiooni toimimine;
- raudteeveo teenuse toimimine (sh reisijate- ja kaubaveo);
- sadamate toimimine, laevaliikluse korraldamine;

- aeronavigatsiooniteenuse ja lennuväljade toimimine.

Uuringus osalevate ETOde poolt osutatavad elutähtsad teenused omavad riigi vaatest olulist tähtsust. Teenuseid tarbib otseselt või nende teenuse katkestusest on kaudselt mõjutatud kogu riigi elanikkond.

Teostatud tööd saame jagada kolmeks peamiseks etapiks:

1) ettevalmistavad tegevused;
2) intervjuude läbiviimine ETOde juures;
3) sisuline kvalitatiivne analüüs.

- **Ettevalmistavad tegevused**

Ettevalmistavate tegevuste käigus tutvuti seadusandliku keskkonnaga ja nõuetega ETOdele teenuse talitluspidevuse tagamiseks. Lisaks viidi läbi sissejuhatavad intervjuud kolme valitud ETKA vastutavate töötajatega.

- **Intervjuud**
  - Intervjuud kolme valitud elutähtsa teenuse toimepidevust korraldava asutuse vastutavate töötajatega.
  - Intervjuud elutähtsa teenuse osutamise eest vastutavate asutuste töötajatega.
  - Intervjuusid ei salvestatud, intervjuu sisu protokolliti kohapeal.
  - Intervjuude protokollid kooskõlastati peale intervjuu läbiviimist kõigi intervjueeritavatega. Intervjuudes osales 24 asutust ning 62 isikut.
  - Intervjuud viidi läbi elutähtsate teenuste osutajate ruumides.
- **Sisuline analüüs**
  - Analüüsiti asutuste dokumente (sh riskianalüüsid ja toimepidevuse plaanid). Dokumentide küsimine toimus koostöös RIAga, analüüs viidi läbi RIA ruumides.

Peamised uuringu käigus ilmnenud tähelepanekud, mis meie hinnangul omavad elutähtsa teenuse toimepidevusele kõige suuremat mõju ja millega tegelemisele tuleks omistada kõrge prioriteet:

- Küsitletud ettevõtetest 37% kasutavad vaid tegevuspõhist riskide hindamist, mille käigus IT riske hinnatakse üldisel tasemel.
- Vaid 33% ettevõtetest on elutähtsa teenuse riskianalüüsi ja toimepidevuse plaane uuendanud hiljem kui 01.01.2015.
- Valdkondlikus vaates on infoturbe riskide haldus hästi korraldatud elektriga varustamise, telekommunikatsiooni ja finantsteenuste valdkonna ettevõtetes.
- Ükski uuringus osalenud ettevõte ei kinnitanud ettevõtte täielikku infosüsteemide turvameetmete süsteemi (ISKE) või ISO 27001 standardi nõuetele vastavust.
- Tuvastasime, et intervjuude läbiviimise ajal eksisteeris IKT-alane välissõltuvus 29% küsitletud ETOdest, sealhulgas olulisel määral 8% ja kriitilisel määral 21% uuringus osalenud ettevõtetest. Kõik uuringus osalenud ettevõtted, kus eksisteerib elutähtsa teenuse välissõltuvus, olid sellega kaasnenud riske enda kohta hinnanud. Ühtse metoodika puudumise tõttu on aga välissõltuvuste dokumenteerituse tase erinev.
- Välisriigis asuvast IKTst sõltuvate ETOde seast suudavad omakorda teenuse osutamise alternatiivlahendusega tagada 57% sõltuvust omavatest ETOdest.

- 12,5% uuringus osalenud ETOdest on vastuolus HOS §40 (1[1]) nõudega, mis sätestab, et juhul kui elutähtsa teenuse toimimist tagavad infosüsteemid asuvad välisriigis, peab ETO tagama elutähtsa teenuse toimepidevuse ka viisil ja vahenditega, mis ei ole sõltuvuses välisriikides paiknevatest infosüsteemidest.
- IKT-alaseid ristsõltuvusi ei ole kõik ETOd piisava detailsusega hinnanud.
- Uuringus osalenud 70% ETOdest ei ole andnud ristsõltuvuste kohta hinnanguid oma riskianalüüsides kõikide uuringu valimis olnud valdkondade lõikes.
- Kõik uuringus osalenud ETOd sõltuvad elektrivarustusest (88% loevad sõltuvust elektritoitest kriitiliseks, 12% oluliseks).
- Kõik uuringus osalenud ETOd sõltuvad sidest, olgu see siis telefoniside, mobiilside või andmeside (46% loevad sõltuvust sidest kriitiliseks, 50% oluliseks).

Peamiste nõrkustena võib esile tuua järgmist:

- Tehniliste vahendite vähesus katkestuste korral alternatiivlahendustega teenuse osutamiseks.
- Riskianalüüsid on koostatud ebaühtlaselt ja erineva detailsusastmega.
- Elutähtsat teenust korraldavate asutuste (ETKA) poolt on teenustasemed määramata.
- Ebapiisav riigipoolne tsentraalne koordineerimine ning ettevalmistus kriisiolukordadeks.
- Stsenaariumipõhiste, erinevaid osapooli, sh ETOsid kaasavaid ühisõppuseid on vähe.
- Pikaajalise elektrikatkestuse puhuks on hetkel tehtud liiga vähe ettevalmistusi.
- Tarvilik on ETO riskianalüüse ja talitluspidevusplaane koostavate inimeste koolitamine.
- Vajalik on ETOde teadlikkuse tõstmine riskide hindamise, küberriskide hindamise jmt alal (juhtkonnast kuni spetsialisti tasemeni välja).
- ETOde arvates tuleb riigil panustada rohkem elutähtsate teenuste osutamise tagamisele ning riskide analüüsimisele.
- Hetkel puudub ühtne infotehnoloogiline lahendus dokumentide operatiivseks vahetamiseks ja hoiustamiseks. Protsess on aeganõudev ja puudub kindlus, kas ETKA ja RIA valduses olev dokumentatsioon kajastab hetkel kehtivat ETOde olukorda.
- Elutähtsate teenuste sõltuvuste hindamiseks ja analüüsimiseks puuduvad ühtsed infotehnoloogilised lahendused. Infot tuleb koguda iga ETO kohta eraldi, kasutades selleks ETO poolt eelnevalt ettevalmistatud dokumentatsiooni ja/või teha selle kohta ETO vastutavatelt isikutelt järelpärimisi.
- Vajalik on järgmistes projektides ETKAl ja/või RIAl analüüsida täpsemalt ETO sõltuvusi oma allhankijatest ja ettevõtetest, kes pakuvad IKT-alaseid teenuseid ETOdele, sest uuringu läbiviimise ajal ei ole neid sõltuvusi ETOd piisavalt detailselt hinnanud.

KPMG soovitused ja tähelepanekud

Tahame rõhutada järgmisi, uuringu käigus ilmnenud tähelepanekuid, mis meie hinnangul omavad elutähtsa teenuse toimepidevusele suurimat mõju ja millega tegelemisele tuleb omistada kõrge prioriteet:

- Selgus, et kõik uuringus osalenud ETOd sõltuvad elektrivarustusest. 88% küsitletud ettevõtetest loeb oma elutähtsa teenuse sõltuvuse elektritoitest kriitiliseks, ilma milleta

teenust pakkuda ei saa ja millele alternatiivse lahenduse pakkumine pikaajaliselt pole võimalik. Elektrikatkestuse korral rakenduvad autonoomsed akutoite süsteemid. ETOd suudavad ajutiselt elektrigeneraatorite abil tagada elektriga varustatuse kõige olulisemates tarbimiskohtades, kuid pole võimalik teenust pakkuda pikaajaliselt ja kõigile tarbijatele. ETOde varustatus elektrigeneraatoritega on ebaühtlane. Soovitame koostada esmalt ETKAde ja seejärel riiklikul tasandil plaanid prioriteetsete elutähtsate teenuste toimimiseks vajalike tarbimiskohtade varustamiseks elektrigeneraatorite ja selleks vajaliku kütusevaruga pikaajalise (rohkem kui 12 tundi kestva) elektrikatkestuse puhuks;

- Intervjuude käigus tuvastasime, et elutähtsa teenuse toimepidevuse korraldajate panustamine elutähtsa teenuse toimepidevuse tagamisse on sõltuvalt valdkonnast väga ebaühtlase tasemega. Soovitame ETKAdel üle kontrollida, et nende alluvuses olevad ETOde parameetrid on vastavuses seadusandlusest tulenevate nõuetega (maksimaalne teenuse katkestuse aeg, lubatud taasteaeg jne). Nõuete puudumise korral tuleb ETKAl nõuded kehtestada. Kui ETOl on need määramata või ei vasta eelpool mainitud nõuetele, siis saab ETO vastava info oma toimepidevusplaanide sisendiks ETKA käest. ETOd ootavad ETKAdelt mitmekülgsemat abi, et ETOdele seadusega määratud toimepidevust puudutavaid kohustusi täita;
- Leidsime, et riskianalüüsi ja toimepidevusplaanide hoiustamisel rakendavad ETOd turvameetmeid väga erineval tasemel. Elutähtsa teenuse riskianalüüsid ning toimepidevuse plaanid sisaldavad tundlikku informatsiooni, millele juurdepääsetavust tuleb piirata. Soovitame ETOdel klassifitseerida antud dokumendid konfidentsiaalseteks ja võtta kasutusele meetmed nende turvaliseks haldamiseks ja hoiustamiseks. Rohkem tähelepanu peab pöörama infoturbe meetmetele dokumentide asutusest välja andmisel ja nende koondamisel ETKAde, Siseministeeriumi ja teiste seotud asutuste poolt;
- Tuvastasime, et intervjuude läbiviimise ajal eksisteeris ETOdel kriitilisi sõltuvusi välisriikides paiknevatest infosüsteemidest. Sellest tulenevalt tekib mittevastavus HOS nõudega, mille kohaselt ETO peab tagama elutähtsa teenuse toimepidevuse viisil ja vahenditega, mis ei ole sõltuvuses välisriikides paiknevatest IKT komponentidest.

Soovitused välissõltuvuste puudujääkide kõrvaldamiseks:

- ETKA koostöös RIA ning Siseministeeriumiga peab kokku leppima, milline osa ETO tegevustest kvalifitseeruvad elutähtsateks teenusteks ning millised teenused on vajalikud lähtuvalt avalikust huvist ja ärilistest eesmärkidest. Elutähtsatele teenustele tuleb kehtestada seadusandlusega konkreetsed toimepidevuse ja käideldavuse nõuded;
- Luua ETOdele soodsad tingimused elutähtsate teenuste osutamisega seotud infosüsteemide majutamiseks planeeritavasse riigipilve.

Soovitused ristsõltuvuste puudujääkide kõrvaldamiseks:

- ETOd peavad läbi viima täiendava analüüsi, milliste objektide varustamine elektriga on kriitiliselt vajalik. Kui koha peal generaator puudub, tuleb luua plaan, kellelt saaks elektrigeneraatoreid ajutiselt laenata. Selleks peab uuringu meeskonna arvates olema Majandus- ja Kommunikatsiooniministeeriumil ja teistel ETKAdel olemas vastavasisuline informatsioon ja kokkulepped, et vajalikul hetkel saaks kiirelt reageerida ning ETOsid aidata;
- uuringus osalenud ETOdest, kelle sidesõltuvus on kriitiline peavad tagama oma olulisematele objektidele dubleeritud sideühendused. Uuringu läbiviijate vaatest peab iga ETO perioodiliselt hindama andmeside ühenduse katkemisest tulenevaid riske ja riski realiseerumise mõjusid. Dubleeritud ühendused tuleb luua selliselt, et ei sõltutaks ühest sideteenuse osutajast ega ühes sidekanalisatsioonis olevatest kaablitest. Lokaalse kaabelsideühenduse katkestuste

riski korral, võib olla otstarbekas kasutada varuvariandina mobiilset andmesidevõrku. Koostöös ETKAde, RIA ja Siseministeeriumiga tuleb kavandada võimalikud riskistsenaariumid, mida ETOd saaks kas iseseisvalt või organiseeritud ühisõppuste käigus testida. Soovitame ETKAdel analüüsida olulisematele elutähtsate teenuse osutamiseks vajalikele objektidele dubleeritud andmeside ühenduste nõuete kehtestamist. Vajadusel tuleb riigi tasandil teha ettepanekud vastavate õigusaktide loomiseks või täiendamiseks.

Soovitused riigipoolse tegevusplaani kohta:

1. Tagada, et kõik vajalikud ja mõjutatud osapooled (peavad eelnevalt olema fikseeritud ETOde ja ETKA poolt toimepidevuse dokumentides) on kursis asjakohase ja ETKA poolt kinnitatud informatsiooniga ETO teenuse katkestusest, sh IT riskide realiseerumisest, mille tulemusena lakkab IKT-komponentide töö.
2. Pakkuda vajadusel abi ETOle teenuse katkestuse taastamise järel info kogumiseks teostatud tegevustest ning võimaldada elektroonilisel teel esmase ülevaatliku intsidendiaruande koostamiseks.
3. Koostöös ETOga intsidendiraporti analüüs, katkestuse põhjuste sügavam uurimine. Tuleviku katkestuste vältimiseks stsenaariumi koostamine (riigipoolsed ohuhinnangud ja stsenaariumid, millega ETOd peaksid arvestama), vajadusel koostada soovitused protsesside muutmiseks. Riik saab siinkohal pakkuda lisaressurssi kogemuste jagamisel.
4. Soovitusliku tegevuskava muudatuste kinnitamine ETO juhatuse tasandil. ETO määrab vastutava isiku, kes hakkab parendustegevuste läbiviimisega tegelema. Riik saaks pakkuda tuge vajaliku protsessi muudatuse läbiviimisel ETOle ning samaaegselt käivitada riigi poolel muudatusega seotud tegevuste läbiviimist.

Soovitused ETOde poolt koostatud materjalide (riskianalüüsid, talitluspidevusplaanid, hädaolukorra lahendamise plaanid jmt) süsteemseks haldamiseks:

- **Soovitame kaaluda ühise turvalise elektroonilise keskkonna loomist. Loodavas keskkonnas saavad elutähtsate teenuste korraldamisega seotud riigiasutused (ETKAd ja muud vajalikud asutused) näha dokumentatsiooni viimaseid versioone ning kasutada analüüsiks teiste ETOde sisendit.** Kuna riskianalüüsides ja toimepidevuse plaanides sisalduv informatsioon on tundlik ja konfidentsiaalne, tuleb erilist tähelepanu loodavas keskkonnas pöörata infoturbemeetmete rakendamisele. Soovitame võimalike riskide vältimiseks eraldada loodav keskkond välisest võrgust. **Soovitame enne arendustööde algust läbi viia eraldi analüüs vastava keskkonna loomisest tekkivate kasude ja võimalike lisanduvate turvariskide tuvastamiseks;**
- **Soovitame luua tsentraalselt hallatava ETOde IKT-komponentide sõltuvuste tabeli, kus tuleb kirjeldada lisaks ETOdele ka allhankijate IKT-komponendid. Kõik allhankijad ei pruugi olla ETOd, aga nende poolt osutatav teenus võib mõjutada olulisel määral ETO IKT-komponentide tööd, seega tuleb vastavas tabelis anda hinnang ka allhankijate süsteemide turvalisusele.** Tsentraalselt hallatav struktuur aitab tagada, et info oleks dokumenteeritud ühtsetel tingimustel;
- ETOdele tuleb luua turvaline krüpteeritud kanal dokumentide üleslaadimiseks ning välistada kõigi muude sidekanalite kasutamine (nt toimepidevuse plaanide saatmine e-kirja manusena, kuna ETOd võivad unustada dokumenti krüpteerida);
- Kõik ETO riskianalüüsid ja talitluspidevusplaanid, mis sisaldavad kolmandate osapooltega (partnerid, teised teenuseosutajad, riigiasutused) seotud tegevusi, tuleb teha vastavatele

osapooltele teatavaks ulatuses, mis kajastab selle osapoole tegevust. ETKA peab igal ajahetkel omama terviklikku ja viimaste täiendustega dokumentatsiooni;

- Hädaolukorras elutähtsate teenuste toimimiseks vajalike tegevusvarude hindamise ja planeerimise võimaldamiseks peab ETOde jaoks koostama ühtse vormi vastava plaani ja taotluse esitamiseks, mis ulatuses ja mis ressursse elutähtsa teenuse pikaajalise katkestuse korral lisaks vajatakse. Ressursikasutuse optimeerimiseks tuleb neid plaane hallata ja ressursse jagada tsentraalselt eelnevalt fikseeritud tingimuste alusel (sh hinnakokkulepped) ning lähtuvalt riigi poolt seatud prioriteetidest;
- Elutähtsa teenuse ja nende komponentide rist-ja välissõltuvuste haldamiseks võib luua infosüsteemi, mis võimaldab analüüsida erinevate teenuste ja teenuste osutamiseks vajalike komponentide vahelisi seoseid. Lisaks peaks vastav süsteem võimaldama erinevaid seoseid visualiseerida. **Arvestades antud uuringu tulemusel ilmnenud nõrkuseid elutähtsa teenuse sõltuvuste kirjeldamisel, dokumenteerimisel ja analüüsimisel, võib väita, et antud süsteemi loomine on vajalik**.

Kontakt

Teet Raidma
IT nõustamisteenuste juht
+372 6 676 814
traidma@kpmg.com

KPMG Baltics OÜ
Narva mnt 5
10117 Tallinn
Estonia

Tel +372 6 268 700
Fax +372 6 268 777

www.kpmg.com