

# SEKTORIAALSE KÜBERRISKIANALÜÜSI KOOSTAMISE JUHEND

## 1. EESMÄRK

Dokumendi eesmärk on kirjeldada Riigi Infosüsteemi Ameti (edaspidi *RIA*) koostatava sektoriaalse küberriskianalüüsi (edaspidi *küberriskianalüüs*) koostamise metoodikat.

## 2. KOOSTAMISE ALUS

Küberriskianalüüsi näol on tegemist üleriigilise riskianalüüsi eelanalüüsiga, mida koostatakse tulenevalt Hädaolukorra seaduse (edaspidi *HOS*) § 9<sup>1</sup> (3). Küberriskianalüüs annab sisendit üleriigilisse riskianalüüsi, aga samamoodi saavad seda kasutada sektori organisatsioonid neid puudutavate asjakohaste küberriskide hindamisel.

Küberriskianalüüs koostatakse kõigi HOS nimetatud teenuste sektorite osas (lisa 1) ja metoodika osas on arvestatud Riigikantselei suuniseid.

## 3. TOIMIVUSE JA VASTAVUSE HINDAMINE

RIA kriitilise infrastruktuuri küberkaitse osakonna riskijuht on selle dokumendi omanikuks ning see on juhendumiseks sektoriaalsete küberriskianalüüside koostamisel.

Dokumendi omanik hindab vähemalt korra aastas dokumendi uuendamise vajalikkust.

## 4. MÕISTED

<b>Alusoh</b>	Eesti Infoturbe Standardi (E-ITS) väljatöötaja poolt riskide kaalutlemisel kasutatud ohud, mis on koos kirjelduste ja näidetega koondatud <a href="#">alusohude kataloogi</a> .
<b>CERT-EE</b>	tuvastab, jälgib ja lahendab Eesti arvutivõrkudes toimuvaid küberintsidente, teavitab ohtudest ning korraldab ennetustegevusi
<b>Enesehindamine</b>	RIA koostatud riskistsenaariumid edastatakse sektori organisatsioonidele hindamiseks, kes oma organisatsiooni põhjal hindavad stsenaariumi realiseerumise tõenäosust ja mõju
<b>ENISA</b>	<i>European Union Agency for Cybersecurity</i>
<b>Riskifaktor</b>	muutuja/näitaja, mis võib eraldi või koos suurendada või vähendada riskistsenaariumi tõenäosuse, mõju ja riskiklassi riskiskoori
<b>Riskiklass</b>	näitab riskistsenaariumist tulenevat riski suurust, kus tõenäosuse ja mõju skooride korrutamise tulemusena leitakse lõplik riskiskoor ja mille alusel jagatakse tulemused vahemikku madal kuni kõrge ja mis näitab riskistsenaariumi riskitaset
<b>Riskiskoor</b>	riskifaktorile määratud numbriline väärtus skaalal 1-5
<b>Sektori organisatsioonid</b>	Hädaolukorra seaduse §36 nimetatud teenuste osas elutähtsa teenuse osutajad ja keskvalitsuste avaliku halduse üksused

## **Üleriigiline riskianalüüs**

on esimene samm riskide hindamise protsessis ja kriisideks vajalike plaanide loomisel. Üleriigiline riskianalüüs keskendub eelkõige julgeolekuohtudele ja suure mõjuga kriisi esile kutsuvatele sündmustele sh küberintsidendile. Üleriigiline riskianalüüs on aluseks kriisideks valmistuvatele asutustele ja isikutele aga ka ühiskonnale tervikuna, et võimaldada hinnata ohte enda toimimisele ja ülesannete täitmisele. Erinevate analüüside koondumist terviklikuks riskipildiks koordineerib Riigikantselei. Üleriigilisest riskianalüüsist saab valdkondlike riskide hindamise, erinevate kriisiplaanide koostamise ja maandamistegevuste planeerimise alus.

## **5. KÜBERRISKIANALÜÜSI KOOSTAMINE**

Küberriskianalüüsi koostamisel järgitakse kindlat struktuuri. Esimeses peatükis kirjeldatakse üldist küberturvalisuse olukorda Euroopas ja Eestis. Samuti antakse ülevaade sektorit peamiselt ohustavatest küberohtudest ja Eestis toimunud intsidentidest. Sektoris toimunud intsidentidest ülevaate koostamiseks kasutatakse CERT-EE registreeritud mõjuga intsidentide statistikat.

Teises peatükis, ehk analüütilises osas, hinnatakse küberriski realiseerumise tõenäosust ja mõju. Selleks koostatakse riskistsenaariumid, mille hindamiseks kasutatakse mitmest allikast tulenevat kombineeritud meetodikat.

Kolmandas peatükis kirjeldatakse küberohtude tulevikusuundasid ja arenguid, mille osas kasutatakse peamise sisendina ENISA publikatsioonides ja töögruppide avaldatud infot.

### **5.1. Küberriskianalüüsi ülesehitus**

Küberriskianalüüside puhul kasutatakse järgmist struktuuri:

1. Olukorra ülevaade (Euroopa/Eesti)
2. Analüüs
  - a. Riskistsenaariumid, mis sisaldavad:
    - i. stsenaarium ja selle kirjeldus
    - ii. alusohud
    - iii. riski realiseerumise võimalikkus Eestis
    - iv. riski realiseerumise tagajärg
    - v. riskiklass ja
    - vi. näited
  - b. Ohud ja nõrkused
  - c. Koondhinnang riski realiseerumise võimalikkusele Eestis
  - d. Sõltuvus teistest teenustest
3. Küberohtude tulevikusuund ja arengud
4. Kokkuvõte
5. Lisad

### 5.1.1. Olukorra ülevaade

Peatüki eesmärk on näidata, millised on peamised sektorit mõjutavad küberohud ja -riskid millega Eesti kriitilise infrastruktuuri organisatsioonid peavad arvestama. Lisaks Euroopas ja mujal maailmas toimuvale annab peatükk ülevaate Eestis enamlevinud ja CERT-EE registreeritud mõjuga küberintsidentidest.

Olukorra ülevaate jaoks kogutakse sisendit erinevatest küberohte ja küberintsidente puudutavatest raportitest (nt. ENISA, RIA poolt avaldatud ülevaated ja raportid) ja muudest RIAle kättesaadavatest allikatest.

### 5.1.2. Analüütiline osa

Analüütiline osa annab ülevaate sektoris enim mõju avaldavatest küberriskistsenaariumitest, nende esinemise tõenäosusest ja mõjust.

#### *Stsenaariumite koostamine ja hindamine*

Riskistsenaariumide koostamise aluseks on enamlevinud ja kriitilist infrastruktuuri peamiselt mõjutavad **küberohud** ning **toimunud intsendid**. Lisas 2 on kirjeldatud küberohud ja riskistsenaariumid, mis on sektorite üleselt samad ja mida sektorile sobivaks kohandades kasutatakse läbivalt erinevate sektorite riskianalüüside puhul. Stsenaariumid, mis on iseloomulikud vaid ühele või paarile sektorile, kirjeldatakse iga küberriskianalüüsi korral eraldi (nt satelliidisignaali segamine). Iga riskistsenaariumi juures tuuakse eraldi välja stsenaariume põhjustavad alusohud. Riskistsenaariumite puhul kasutatakse alusohude määramiseks [E-ITS alusohude kataloogi](#).

Riskistsenaariumite ilmestamiseks kasutatakse sektorikohaseid avalikult kättesaadavate küberintsidentide näiteid nii Eestist kui ka mujalt maailmast. CERT-EEle raporteeritud intsendid on konfidentsiaalsed ja seetõttu neid stsenaariumite puhul näidetena ei kasutata.

Stsenaariumite puhul hinnatakse nende realiseerumise tõenäosust ja mõju, mille koostoimes määratakse riskiklass. Hindamise aluseks on sektori organisatsioonide enesehindamise tulemused RIA koostatud riskistsenaariumite vastu ja toimunud mõjuga küberintsendid. Riskistsenaariumite analüüsi ja hindamise tulemusena selgitatakse välja sektori organisatsioone peamiselt ohustavad *alusohud* ja *nõrkused*.

Sektori küberriski realiseerumise võimalikkuse koondtulemuse puhul arvestatakse lisaks üksikute stsenaariumite hinnangule IP-põhise *Risk Monitoring Service* tulemusi, samuti muud teavet, mis mõjutab küberriski realiseerumise võimalikkust Eestis (näiteks teiste riikide poolt välja antud sektoriaalsed ohuhinnangud, tuvastatud sektoriüleised nõrkused jmt).

Täpne riskistsenaariumite hindamise mudel on kirjeldatud lisas 3.

Lisaks kirjeldatakse küberriskianalüüsis *teenuse sõltuvust teistest elutähtsatest teenustest* ja antakse *ülevaade küberohtude tulevikusuundadest ja muutustest*.

### 5.1.3. Küberriskianalüüsi lisad

Sektoriaalse küberriskianalüüsi lisad on:

Lisa 1. Riskistsenaariumite (R1-Rn) koondtabel

Lisa 2. Stsenaariumi realiseerumise tõenäosuse hindamine

Lisa 3. Stsenaariumi realiseerumise tagajärje hindamine<sup>1</sup>

Lisa 4. Riskiklassid

Lisa 5. Sektori riskistsenaariumide riskimaatriks

Lisa 6. Sektori stsenaariumipõhiste ohtude koondülevaade

## **6. RISKIANALÜÜSI UUENDAMINE**

Kuna riskid on pidevas muutuses, siis hinnatakse küberriskianalüüsi ajakohasust vähemalt kord aastas või siis, kui toimuvad varasemat hinnangut mõjutavad olulised muutused (nt geopoliitilise olukorra muutumisel või toimunud intsidentide põhjal).

## **7. KÜBERRISKIANALÜÜSI AVALIKUSTAMINE**

RIA teavitab valminud ja uuendatud küberriskianalüüsidesid sektori organisatsioonidele. Samuti avaldatakse sektoriaalsed küberriskianalüüsid RIA [kodulehel](#), kus need on kättesaadavad kõigile huvilistele.

---

<sup>1</sup> [https://www.riigiteataja.ee/aktiis/1310/7202/1002/VV\\_75m\\_lisa3.pdf#](https://www.riigiteataja.ee/aktiis/1310/7202/1002/VV_75m_lisa3.pdf#)

**Lisa 1. CER Direktiivist tulenevad ja hädaolukorra seaduses nimetatud teenused, mille osas koostatakse sektoriaalne küberriskianalüüs**

<b>Sektor</b>	<b>HOS nimetatud teenus</b>
Energeetika	elektriga varustamine
	kaugküttega varustamine
	vedelkütusega varustamine
	maagaasiga varustamine
Side	andmesideteenuse toimimine
	telefoniteenuse toimimine
	mobiiltelefoniteenuse toimimine
Digitaristu	elektrooniline isikutuvastamine ja digitaalne allkirjastamine
Lennutransport	lennuväljade toimimine
	aeronavigatsiooniteenuse toimimine
Veetransport	sadamate toimimine
Maantee	riigitee sõidetavuse tagamine; kohaliku tee sõidetavuse tagamine
Raudtee	avaliku raudtee toimimine
Finantssektor	krediiditehingute töötlemine
	sularaharinglus
	makseteenus
Tervishoid	tervishoiuteenuste toimimine
	ravimitega varustamine
Vesi- ja kanalisatsioon	veega varustamine ja kanalisatsioon
Avaliku halduse üksused	keskvalitsus <sup>2</sup>
Kosmos	n/a
Toiduainete tootmine, töötlemine ja turustamine	toiduga varustamine

<sup>2</sup> Liikmesriigi õiguses määratletud keskvalitsuste avaliku halduse üksused

## Lisa 2. Riskistsenaariumite aluseks olevad küberohud ja näidiskitsenaariumid

<b>Küberoht 1</b>	<b>Hajutatud teenustökestusrünnak (DDoS)</b>
<b>Kirjeldus</b>	DDoS rünnakud on hästi nähtavad küberrünnakud, mis ujutavad võrgu või süsteemi liiklusega üle nii, et need muutuvad kättesaamatuks. DDoS rünnakuid viivad enamast läbi vaenulike riikide toetatud rühmitused eesmärgiga vaigistada aktiviste või häirida välisriigi valitsusasutuste tööd, organiseeritud kuritegevuse rühmitused nt väljapressimise eesmärgil, häktivistide rühmitused ja "script kiddies" eesmärgiga toetada vaenuliku riigi toetatud rühmituse tegevust. DDoS rünnakute vastase kaitse tase ja ettevalmistus on väga erinev.
<b>Riskistsenaarium 1 (R1). Suunatud teenustökestusrünnakud häirimaks sektori organisatsioonide tööd</b>	
<i>Ideoloogiliselt motiveeritud häkkerid (häktivistid) võtavad sihikule (...)sektori organisatsioonid. Suuremahulise DDoS rünnaku käigus häiritakse sektoris tegutsevate organisatsioonide tavapärase tööd. DDoS varjus kaardistatakse organisatsioonide süsteeme ja tuvastatakse mitmeid turvaauke, mida kasutatakse hiljem suunatud rünnakute toimepanemiseks.</i>	
<b>R1 seotud alusohud</b>	G 0.14; G 0.18; G 0.23; G 0.25; G0.28; G 0.29; G 0.30; G 0.31; G 0.40; G 0.47
<b>Küberoht 2</b>	<b>Lunavararünnak</b>
<b>Kirjeldus</b>	Lunavararünnaku eesmärgiks on failide ja muude andmete krüpteerimine ning ohvrilt dekrüpteerimisvõtme eest lunavara nõudmine. Lunavararünnakud on küberturvalisuse maastikul domineerinud viimased paar aastat. <b>Hävitusvara</b> on sageli oma olemuselt sarnane kasutatavate ründemeetodite/tehnikate mõttes, aga andmete krüpteerimise asemel need lihtsalt kustutatakse (või krüpteeritakse võtmega, mis kustutatakse). Lunavararünnakuid teevad tavaliselt organiseeritud kuritegevuse rühmitused, hävitusvara rünnakuid vaenuliku riigi toetatud või häktivistide rühmitused. Suureks murekohaks on keeruka hävitusvara (nagu NotPetya) kasutamise risk, mis toimib nagu lunavara, aga hävitab võrguoperaatorite infrastruktuuris olevad andmed ja süsteemid. Laiaulatuslik andmeid hävitav pahavara või lunavararünnak keskse infrastruktuuri või selle aluseks olevate varade vastu võib endaga kaasa tuua väga pika taasteaja.
<b>Riskistsenaarium 2 (R2). Lunavararünnak, mille tulemusena saab häiritud tavapärane töökorraldus ning lekivad klientide ja töötajate andmed</b>	
<i>Kurjategijad korraldavad küberrünnaku tungides organisatsiooni IT-süsteemidesse. Lisaks häiretele tavapärase tööprotsessis, varastatakse töötajate ja klientide isikuandmed. Organisatsioon keeldub lunavara maksimisest ja neil õnnestub süsteemide töö taastada kuu peale kompromiteerimist. Tulenevalt manuaalsest tööprotsessist ja IT-süsteemide taastamisest on tavapärane töö taasteperioodi jooksul häiritud. Lunavara maksimisest keeldumise tagajärjel müüvad küberkurjategijad töötajate ja klientide andmed tumeveebis edasi.</i>	
<b>R2 seotud alusohud</b>	G 0.18; G 0.19; G 0.21; G 0.22; G 0.23; G 0.27; G 0.28; G 0.29; G 0.30; G 0.31; G 0.32; G 0.33; G 0.34; G 0.39; G 0.41; G 0.45; G 0.46; G 0.47
<b>Küberoht 3</b>	<b>Sisevõrku tungimine, ebaseadusliku juurdepääsu loomine</b>
<b>Kirjeldus</b>	Võrku sissetungimist kasutatakse spionaažiks, andmevargusteks või edasiste küberrünnakute ettevalmistamiseks. Võrku tungimist võib olla raske tuvastada ja selle tagajärjed võivad olla pikaajalised ning ettearvamatud. Tavaliselt tungivad sisevõrku spionaaži eesmärgil vaenuliku riigi toetatud rühmitused, kuid ka organiseeritud kuritegevuse rühmitused võivad sisevõrku tungida ja kasutada saadud väärtuslikku teavet ohvrilt väljapressimiseks. Infot kasutatakse edasiste küberrünnakute planeerimiseks või müüakse saadud andmed tumeveebis edasi.
<b>Riskistsenaarium 3 (R3). Küberkurjategijad kasutavad ära tarkvara turvanõrkust ja tungivad organisatsiooni sisevõrku</b>	
<i>Küberkurjategijad kasutavad ära paikamata jäänud turvanõrkust laialdast kasutust leidvas tarkvaras, mille abil kompromiteeritakse organisatsiooni sisevõrk. Seoses rünnakuga saab häiritud teenuse pakkumiseks vajalike süsteemide töö, aga esineb katkestusi ka põhiteenuse osutamises.</i>	
<b>R3 seotud alusohud</b>	G 0.18; G 0.21; G 0.23; G 0.28; G 0.29; G 0.31; G 0.41; G 0.47
<b>Riskistsenaarium 4 (R4). Kurjategijad saavad kaughalduslahenduse kaudu ligipääsu organisatsiooni sisevõrku ja tekitavad häireid tavapärase tööprotsessis</b>	
<i>Küberkelmid saavad ebaturvaliselt seadistatud kaughalduslahenduse kaudu ligipääsu organisatsiooni sisevõrku, krüpteerivad andmed organisatsiooni serveris ja nõuavad lunaraha krüptovaluutas. Organisatsioonil on krüpteeritud andmetest varukoopiaid olemas, aga tavapärase töö taastamiseks kulub kaks nädalat. Seega on tavapärane töö tugevalt häiritud.</i>	

<b>R4 seotud alusohud</b>	G 0.18; G 0.23; G 0.27; G 0.28; G 0.29; G 0.31; G 0.39; G 0.41; G 0.45; G 0.46; G 0.47
<b>Riskistsenaarium 5 (R5). Küberkurjategija tungib <u>organisatsiooni</u> sisevõrku ja manipuleerib käidutehnoloogia tööd</b>	
<i>Küberkurjategijad tungivad sihitud õngitsuse tulemusena <u>organisatsiooni</u> sisevõrku ja võtavad käidutehnoloogia (nt SCADA) enda kontrolli alla. Kurjategijad manipuleerivad süsteemi selliselt, et põhiteenuse osutamine katkeb mitmeks tunniks. Täiendava segaduse tekitamiseks rünnatakse <u>organisatsiooni</u> veebilehte ja e-teenuste tööd teenustökestusrünnetega.</i>	
<b>R5 seotud alusohud</b>	G 0.18; G 0.21; G 0.23; G 0.27; G 0.29; G 0.30; G 0.36; G 0.39; G 0.40; G 0.41; G 0.45; G 0.46; G 0.47
<b>Küberoht 4</b>	<b>Lubamatu sisenemine/sabotaaz</b>
<b>Kirjeldus</b>	<p><b>Lubamatult hoonesse või territooriumile sisenejatega</b> võivad kaasuda mitmesugused ohud, näiteks teabe või IT-süsteemide vargus või manipuleerimine. Oskuslike rünnete puhul on otsustav see ajavahemik, mille vältel saab ründaja segamatult ja sihipäraselt tegutseda. Tihti varastab ründaja väärtuslikke IT-komponente või muid varasid, mida on kerge müüa, kuid sissemurdmise eesmärgiks võib mh olla ka konfidentsiaalse teabe juurde pääsemine, selle manipuleerimine või äriprotsesside häirimine. Territooriumile loata sisenemine võib tekitada mitut liiki kahju. Akende ja/või uste lahtimurdmine kahjustab neid ning need tuleb parandada või asendada. Varastatud, kahjustatud või hävitatud seadmed või komponendid tuleb parandada või asendada. Kahju võib tekkida teabe või rakenduste konfidentsiaalsuse, tervikluse või käideldavuse rikkumisest.</p> <p><b>Sabotaaz</b> on objektide või protsesside kuritahtlik manipuleerimine või rikkumine eesmärgiga tekitada ohvrile kahju. Eriti atraktiivsed sihtmärgid võivad olla organisatsiooni arvutikeskused või sidekanalid, sest siin saab suhteliselt väheste vahenditega saavutada ranga tagajärje. Käitushäiringute esilekutsumiseks saavad arvutikeskuse keerukat taristut manipuleerida eelkõige sisemised, aga ka välised isikud. Eriti puudutab see puudulikult kaitstud hoone- ja sidetehnilist taristut ning tsentraalseid varustussõlmi, mis korralduslikel või tehnilistel põhjustel võivad olla järelevalveta ning kõrvalistele isikutele kergelt ja märkamatu kättesaadavad.</p>
<b>Riskistsenaarium 6 (R6). Ründaja saab tulenevalt ebapiisavatest füüsilistest turvameetmetest ligipääsu <u>organisatsiooni</u> kriitilistele süsteemidele</b>	
<i><u>Organisatsiooni</u> läbipääsusüsteemis kasutatavad uksekaardid on ebaturvalised ja hõlpsasti kopeeritavad. Kriitiliste süsteemide juurde viivad ukсед avanevad uksekaardiga ilma täiendava PIN-koodita. Ründaja siseneb kopeeritud uksekaardiga <u>organisatsiooni</u> ruumidesse, leiab SCADA operaatori töökoha ja manipuleerib SCADA kaudu kontrollitavaid parameetreid.</i>	
<b>R6 seotud alusohud</b>	G 0.14; G 0.18; G 0.20; G 0.21; G 0.23; G 0.29; G 0.30; G 0.34; G 0.41; G 0.44
<b>Küberoht 5</b>	<b>Tarneahela rünnak</b>
<b>Kirjeldus</b>	Tarneahela rünnak koosneb tavaliselt kahest sammust. Esmalt rünnatakse tarnija võrku või süsteemi. Teises etapis rünnatakse tegelikku sihtmärki. Tarneahela rünnakuid kasutavad vaenuliku riigi toetatud häktivistide rühmitused, samuti organiseeritud kuritegevuse rühmitused või häktivistide grupeeringud. Tarneahela rünnakutel võib olla suur mõju, kuna need võimaldavad ründajatel võtte sihikule palju erinevaid operaatoreid, kes on seotud sama teenusepakkujaga. Tarneahela rünnakud on ründajate jaoks atraktiivsed ka teisel põhjusel, nimelt võivad ründajad olla võimelised mööda hiilima sideoperaatori või teenusepakkuja kaitsemehhanismidest võttes esmalt sihikule tarnija, kellel on võibolla nõrgem kaitse- ja tuvastamisvõime.
<b>Riskistsenaarium 7 (R7). Käidutehnoloogia süsteemide kahjustamine pahatahtliku koodiga põhjustab <u>organisatsioonis</u> intsidendi</b>	
<i>Küberkurjategijad tungivad käidutehnoloogia süsteemide hooldustöök kasutatavasse sülearvutisse (kas läbi nakatatud USB, e-kirja, internetist allalaetud tarkvara vms), ja käivitavad seal pahatahtliku koodi. Kui sülearvuti ühendatakse, siis levib pahatahtlik kood sealt edasi käidutehnoloogia süsteemidesse ja võrkudesse. Selle tulemusena on kurjategijatel võimalik tehnajuhtimissüsteem (ICS) distantilt oma kontrolli alla võtta. Mõjutades käidutehnoloogia süsteemi lõppseadmeid tekitavad kurjategijad intsidendi, mille tulemusena saab kahjustada <u>organisatsiooni</u> infrastruktuur ja ohtu seatakse seal viibivate inimeste elu ja tervis.</i>	
<b>R7 seotud alusohud</b>	G 0.18; G 0.21; G 0.23; G 0.28; G 0.29; G 0.39; G 0.47

<b>Küberoht 6</b>	<b>Sisemine oht</b>
<b>Kirjeldus</b>	Teenuspakkujaid võivad mõjutada siseringi isikud, kes tegutsevad vaenuliku riigi toetatud rühmituse või organiseeritud kuritegeliku grupeeringu agendina. Nimetatud rünnakute mõju sõltub sellest, millised ligipääsud ja õigused on siseringi isikul tundlikele andmetele ja kriitilisele infrastruktuurile. Risk võib olla suurem, kui operaatorid tellivad peamisi äriprotsesse allhanke korras kolmandatest riikidest.
<b>Riskistsenaarium 8 (R8). Hooletu töötaja tõttu tungivad küberkurjategijad <u>organisatsiooni</u> sisevõrku ja nakatavad selle lunavaraga</b>	
<i>Organisatsiooni</i> töötaja korduvkasutab oma tööandja süsteemide parooli erinevates avalikes keskkondades. Andmelekkete tulemusena avalikus süsteemis lekivad tema paroolid ja kurjategijad tungivad töötaja VPN konto kaudu <u>organisatsiooni</u> sisevõrku. Ründajad varastavad tundlikke andmeid ja nakatavad sisevõrku lunavaraga. Dekrüpteerimisvõtme saamiseks esitatakse <u>organisatsioonile</u> mitme miljoni euro suurune lunavaranõue, mis tuleb tasuda krüptovaluutas.	
<b>R8 seotud alusohud</b>	G 0.18; G 0.19; G 0.23; G 0.29; G 0.30; G 0.31; G 0.39; G 0.46; G 0.47
<b>Riskistsenaarium 9 (R9). Vaenuliku riigi esindaja värbab organisatsiooni rahulolematu töötaja, kes lekib konfidentsiaalset infot</b>	
<i>Organisatsioonis</i> võtmepositsiooni omav töötaja on juba pikalt demotiveeritud ja tunneb, et tema panust ei hinnata vääriliselt. Vaenuliku riigi agent läheneb töötajale ja pakub talle „teenete“ eest paremat tööd ja väärilist palka. Oma töös pettunud töötaja otsustabki eirata <u>organisatsiooni</u> siseseid turvapoliitika ja edastab konfidentsiaalset teavet <u>organisatsiooni</u> tööprotsesside, IT süsteemide ja nende arhitektuuri kohta vaenuliku riigi agendile. Kogutud info alusel planeerivad vaenuliku riigi küberüksused manipuleerida <u>organisatsiooni</u> infosüsteeme eesmärgiga külvata segadust ja tekitada finantskahju.	
<b>R9 seotud alusohud</b>	G 0.14; G 0.16; G 0.18; G 0.19; G 0.29; G 0.32; G 0.35; G 0.42; G 0.46
<b>Riskistsenaarium 10 (R10). Teenuse häirimine (endise) pahatahtliku töötaja/teenusepakkuja töötaja poolt</b>	
<i>Kriitilistele süsteemidele ligipääse omav võtmetöötaja eksib korduvalt siseprotseduuride vastu, mistõttu tema tööleping lõpetatakse. Tulenevalt <u>organisatsiooni</u> puudulikust infoturbe korraldusest jäetakse tema kaugjuurdepääs kriitilistele süsteemidele peale töölepingu lõpetamist eemaldamata. Töötaja on vallandamise pärast väga pahane ja tahab oma endisele tööandjale kätte maksta, seetõttu tungib ta <u>organisatsiooni</u> sisevõrku ja kustutab seal hulga vajalikke dokumente ja andmeid, millest tagavarakoopiad puuduvad. Seetõttu on tavapärase tööprotsessi pikalt häiritud.</i>	
<b>R10 seotud alusohud</b>	G 0.14; G 0.16; G 0.18; G 0.19; G 0.29; G 0.32; G 0.42; G 0.46
<b>Küberoht 7</b>	<b>Õngitsemine</b>
<b>Kirjeldus</b>	<b>Õngitsemine</b> ehk <i>phishing</i> on inimpsüühikaga manipuleerimise üks viise, millega üritatakse arvutikasutaja viia nii kaugele, et ta annab kurjategijale ise oma juurdepääsuandmed, paroolid, krediitkaardi rekvisiidid ja muu turvakriitilise informatsiooni. Õngitsused jagunevad laias laastus kaheks – kontoõngitsused (kasutajanimed ja salasõnad) ja pangaandmete õngitsused (krediitkaartide andmed, PIN-koodid). Viimaste puhul on kahju kiire tulema, paroolilekke tagajärjed võivad ilmned kuude või aastate pärast.
<b>Riskistsenaarium 11 (R11). Õngitsemise tulemusel tungib küberkurjategija <u>organisatsiooni</u> sisevõrku ja nõuab lunaraha krüpteeritud andmete eest</b>	
<i>Organisatsiooni</i> juht edastab töötajatele e-kirja infoga, et organisatsioon on langenud küberrünnaku ohvriks, mistõttu palutakse kõigil töötajatel kiiresti muuta meilikonto paroolid. Kirjale on lisatud vastava keskkonna link. Hiljem selgub, et <u>organisatsiooni</u> tegevjuhi meilikonto on kompromiteeritud ja seda on kasutatud õngitsusründe toimepanemiseks, mille tulemusena saavad kurjategijad ligipääsu <u>organisatsiooni</u> infosüsteemidele. Rünnakule järgneb lunarahanõue.	
<b>R11. seotud alusohud</b>	G 0.19; G 0.20; G 0.22; G 0.23; G 0.29; G 0.30; G 0.31; G 0.36; G.0.39; G 0.47

### Lisa 3. Riskistsenaariumide ja sektori koondriski hindamise meetodika

Riskihindamise mudeli peamine eesmärk on riski kvantifitseerimine ja mõõtmine. Hinnatakse riskistsenaariumi realiseerumise tõenäosust, mõju ja määratakse stsenaariumile riskiklass. Erinevate riskifaktorite koostoimes antakse koondhinnang küberriski realiseerumise võimalikkusele Eestis.

Mudeli koostamisel ja riskifaktorite valikul on kaalutud järgmiseid allikaid:

- 1) sektoris tegutsevate organisatsioonide enesehindamine riskistsenaariumite vastu;
- 2) sektoris toimunud ja CERT-EE registreeritud mõjuga intsidendid;
- 3) *Risk Monitoring Report* IP põhise monitooringu tulemused;
- 4) sektori organisatsioonide kohta kogutud teave (küberturvalisuse olukord, turvalisuse hindamise tulemused, jm RIA-le teatavaks saanud ettevõtte/asutuse küberturvet puudutav teave).

Hindamismudeliga määratakse riskifaktorite osas skoorid ja kaalud, mille koosmõjus leitakse iga stsenaariumi osas (all)sektorikohane tõenäosuse, mõju ja riskiklassi lõplik hinnang ning sektoriülene küberriski realiseerumise võimalikkuse koondhinnang.

#### Sektoris tegutsevate organisatsioonide enesehindamine

Käesoleva juhendi lisa 2 olevad riskistsenaariumid kohandatakse ja edastatakse hindamiseks sektori elutähtsa teenuse osutajatele, kes hindavad riskistsenaariume oma organisatsiooni vaatest vastavalt käesoleva juhendi lisadele 4 (*Stsenaariumi realiseerumise tagajärje hindamine*) ja 5 (*Stsenaariumi realiseerumise mõju hindamine*). Antud hinnangud teisendatakse skoorideks skaalal 1-5, kus 1 tähistab väiksemat võimalikku tõenäosust ja mõju ning 5 suurimat.

#### Riskistsenaariumide kaalutud keskmise arvutamine

RIA kogub üksikute organisatsioonide riskistsenaariumite enesehindamise tulemused kokku ja leiab iga stsenaariumi osas selle realiseerumise tõenäosuse ja mõju kaalutud keskmise hinnangu. Kaalutud keskmise puhul arvestatakse osakaaluna organisatsiooni suurust (tabel 1), kuna organisatsioonid on erineva suurusega ja seega on ka võimalik mõju riskistsenaariumi realiseerumise korral erinev.

Ettevõtte kategooria	Töötajate arv (aastane tööühik)	Aastakäive	Aastabilansi kogumaht	Osakaal
Suur (S)	250 ja enam	või üle 50 miljoni €	või üle 43 miljoni €	40% (0,4)
Keskmine (K)	vähem kui 250	ja ei ületa 50 miljonit €	või ei ületa 43 miljonit €	30% (0,3)
Väike (V)	vähem kui 50	ja ei ületa 10 miljonit €	või ei ületa 10 miljonit €	20% (0,2)
Mikro (M)	vähem kui 10	ja ei ületa 2 miljonit €	või ei ületa 2 miljonit €	10% (0,1)

Tabel 1. Organisatsiooni suurusest<sup>3</sup> tulenevalt määratud osakaalud enesehindamise tulemuste kaalutud keskmise leidmiseks

<sup>3</sup> Väike- ja keskmise suurusega ettevõtja (VKE) definitsiooni selgitus vastavalt Euroopa Komisjoni määruse 800/2008/EÜ lisa 1-le

Organisatsioonide enesehindamise kaalutud keskmise arvutamiseks kasutatakse tabelit 2.

Riski- stsenaarium	Organisatsioon	Enesehindamine		
		Osakaal	Tõenäosus	Mõju
R1-Rn	Org 1-Org n	0,1-0,4	1-5	1-5
<i>R1-Rn skoor kokku*</i>			<i>1-5</i>	<i>1-5</i>

Tabel 2. Organisatsioonide enesehindamise kaalutud keskmise määramine

\*Riskistsenaariumi skoor kokku – organisatsioonide enesehindamise tulemuste kaalutud keskmine skoor

### Riskistsenaariumite tõenäosuse skoori täpsustamine

Järgmise sammuna täpsustatakse riskistsenaariumite hindamisel stsenaariumite tõenäosuse skoori tulenevalt toimunud mõjuga intsidentidest. Juhul, kui sektoris on toimunud stsenaariumikohaseid mõjuga intsidente, siis sõltuvalt esinenud mõjuga intsidentide hulgast suureneb tõenäosuse enesehindamise kaalutud keskmine skoor 0,5 või 1 punkti ülespoole. Juhul, kui mõjuga intsidente ei ole toimunud, jääb skoor muutumatuks. Kahes etapis määratud riskifaktorite skooride põhjal leitakse riskistsenaariumi (all)sektori kohane tõenäosuse ja mõju hinnang ning määratakse sellest tulenevalt riskiklass.

Riskistsenaariumite tõenäosuse skoori täpsustamiseks kasutatakse tabelit 3. Tõenäosuse skooride puhul tõstavad toimunud mõjuga intsidendid riskistsenaariumi enesehindamise kaalutud keskmist skoori, aga lõplikud skoorid jäävad vahemikku 1-5, st lõplik skoor >5 =5.

R1-Rn	Tõenäosus		Mõju	Riskiklass
<b>Enesehindamine</b>	1-5			1-25
<b>Mõjuga intsidendid</b>	>/=10	1	1-5	
	<10	0,5		
	Ei	0		
<b>R1-Rn kokku:</b>	<b>1-5</b>		<b>1-5</b>	<b>1-25</b>

Tabel 3. Riskifaktorite skoorid riskistsenaariumite enesehindamise tulemuste täpsustamiseks

Erinevalt organisatsioonide enesehindamisest kasutab RIA (all)sektori tõenäosuse hindamiseks lisas 6 ja riskiklassi määramiseks lisas 7 asuvat tabelit.

### Küberriski realiseerumise võimalikkuse koondhinnangu määramine

Üldise sektoriülese küberriski realiseerumise tõenäosuse puhul arvestatakse enesehindamise ja toimunud intsidentide riskifaktoritele lisaks Risk Monitoring Service IP põhise monitooringu tulemusi jm RIA-le teadaolevat infot, mis sektori küberriski realiseerumise koondhinnangut mõjutab.

RM turvareiting tõstab või langetab sektoriülese küberriski realiseerumise tõenäosuse skoori, aga lõplik skoor jääb vahemikku 1-5, st lõplik skoor <1 = 1 ja >5 =5.

Sektoriülese küberriski realiseerumise tõenäosuse hindamiseks kasutatakse tabelit 3.

<b>Küberriski realiseerumise tõenäosuse koondhinnang</b>		
<b>R1-Rn keskmine tõenäosus:</b>		<b>1-5</b>
RM**	<630	1
	640-730	0,5
	>740	-0,5
<b>Koondtulemus</b>		<b>1-5</b>

Tabel 3. Riskifaktorite skoorid küberriski realiseerumise võimalikkuse koondtulemuse arvutamiseks

\*\*RM – Risk Monitoring Service turvareiting

<b>Turvareiting</b>	<b>Tase</b>	<b>Selgitus</b>
<630	põhitase	5x suurem tõenäosus kogeda andmetega seotud rikkumisi, kui üksustel, kelle turvareiting on 700 ja kõrgem
640-730	kesktase	Madalam turvareiting ja suurenenud tõenäosus andmetega seotud rikkumiseks
>740	kõrgtase	

Tabel 4. BitSight Risk Monitoring Service turvareitingu tasemed

**Lisa 4. Stsenaariumi realiseerumise tagajärje hindamine<sup>4</sup>**

Raskusaste	Tagajärje hindamise kriteeriumid		
	Teenuse osutamise maht	Maine	Majanduslik
<b>katastroofiline</b>	Teenuse osutamine on takistatud 80-100% ulatuses kriitilise tegevuse äärmiselt tõsise häire tõttu	Püsivalt mitu kuud kestev avalikkuse ja meedia äärmiselt vaenulik tähelepanu	Plaanitud laekumiste vähenemine >30%, kasumi vähenemine >30% võrra
<b>väga raske</b>	Teenuse osutamine on takistatud 50-80% ulatuses kriitilise tegevuse väga tõsise häire tõttu	Nädalaid kestev märkimisväärne avalikkuse ja meedia negatiivne tähelepanu	Plaanitud laekumiste vähenemine 20-30%, kasumi vähenemine 15-20% võrra
<b>raske</b>	Teenuse osutamine on takistatud 30-50% ulatuses kriitilise tegevuse raske häire tõttu	Päevi kestev ja korduv avalikkuse ja meedia negatiivne tähelepanu	Plaanitud laekumiste vähenemine 5-10%, kasumi vähenemine 5-15% võrra
<b>kerge</b>	Teenuse osutamine on takistatud 10-30% ulatuses kriitilise tegevuse kerge häire tõttu	Päevi kestev avalikkuse ja meedia negatiivne tähelepanu	Plaanitud laekumiste vähenemine 1-5%, kasumi vähenemine 1-5% võrra
<b>vähetahtis</b>	Teenuse osutamine on takistatud 0-10% ulatuses kriitilise tegevuse pisihäire tõttu või häireid ei ole	Avalikkuse negatiivne tähelepanu puudub või on minimaalne	Plaanitud laekumiste vähenemine <1%, kasumi vähenemine <1% võrra

<sup>4</sup> [https://www.riigiteataja.ee/aktiivisa/1310/7202/1002/VV\\_75m\\_lisa3.pdf#](https://www.riigiteataja.ee/aktiivisa/1310/7202/1002/VV_75m_lisa3.pdf#)

## Lisa 5. Stsenaariumi realiseerumise mõju hindamine<sup>5</sup>

<b>Stsenaariumi realiseerumise tõenäosus</b>	<b>Kriteerium</b>
Väga suur	> 99% tõenäosusega Juhtub sageli Võib juhtuda päevade ja nädalate jooksul
Suur	> 50% tõenäosusega Võib kergesti juhtuda Võib juhtuda nädalate ja kuude jooksul
Keskmine	> 10% tõenäosusega On varem juhtunud Võib juhtuda aasta jooksul
Väike	> 1% tõenäosusega Ei ole juhtunud, kuid võib juhtuda Võib juhtuda aastate pärast
Väga väike	< 1% tõenäosusega On tõenäoline ainult ekstreemsetes tingimustes Võib juhtuda korra 100 aasta jooksul

<sup>5</sup> Kasutatakse organisatsiooni enesehindamise puhu [https://www.riigiteataja.ee/aktiilisa/1310/7202/1002/VV\\_75m\\_lisa2.pdf#](https://www.riigiteataja.ee/aktiilisa/1310/7202/1002/VV_75m_lisa2.pdf#)

## Lisa 6. Stsenaariumi realiseerumise mõju hindamine <sup>6</sup>

<b>Stsenaariumi realiseerumise tõenäosus</b>	<b>Kriteeriumiks on realiseerumise tõenäosus Eestis järgmise 2 aasta jooksul</b>
Väga suur	kindlasti juhtub, küsimus vaid millal (81–100%)
Suur	väga tõenäoline (61–80%)
Keskmine	tõenäoline (41–60%)
Väike	vähe tõenäoline (21–40%)
Väga väike	ebatõenäoline (0–20%)

---

<sup>6</sup> RIA kasutab (all)sektori riskistsenaariumi ja küberriski realiseerumise tõenäosuse koondhinnangu andmisel Riigikantselei poolt antud metoodikat

## Lisa 7. Riskiklassi määramine

TAGAJÄRG						
TÕENÄOSUS		vähetahtis	kerge	raske	väga raske	katastroofiline
	väga suur	Keskmine (5)	Oluline (10)	Kõrge (15)	Kõrge (20)	Kõrge (25)
	suur	Keskmine (4)	Oluline (8)	Oluline (12)	Kõrge (16)	Kõrge (20)
	keskmine	Madal (3)	Keskmine (6)	Oluline (9)	Oluline (12)	Kõrge (15)
	väike	Madal (2)	Keskmine (4)	Keskmine (6)	Oluline (8)	Oluline (10)
	väga väike	Madal (1)	Madal (2)	Madal (3)	Keskmine (4)	Keskmine (5)

Riskiskoor	Riskiklass
Kuni 3	madal
4 kuni 7	keskmine
8 kuni 14	oluline
15 kuni 25	kõrge