RISKIANKEET

1. Küberintsident

2. Riskianalüüsi koostanud juhtiv asutus	**3. Riskianalüüsi kinnitamise kuupäev:** 18.05.2018
Riigi Infosüsteemi Amet	**4. Viide riskianalüüsile:** Riigi Infosüsteemi Ameti peadirektori 18.05.2018 käskkiri nr 1.1-2/18-056

5. Kokkuvõte toimunud sündmustest

Viimaste aastate üleilmseid sündmusi hinnates saab rääkida küberintsidentide üha kaalukamast mõjust riigi toimimiseks olulistele ja elutähtsatele teenustele.

Ehkki otseselt küberintsidendist põhjustatud hädaolukorda Eestis tekkinud ei ole, on ulatusliku küberintsidendi oht kasvav kogu maailmas ning oskusteave, kuidas rünnata, areneb pidevalt. Hädaolukorraga võivad kaasneda suured varalised ja maine kahjud. Küberintsidendi abil on võimalik destabiliseerida ühiskonnakorraldust, võib kaduda usaldus oluliste e-teenuste ja seda võimaldava avaliku võtme infrastruktuuri turvalisuse vastu. Küberrünnaku tulemusena teatud sidekanalite halvamisega on võimalik ära lõigata paljud inimeste jaoks vajalikud teenused, mille tagajärjel võib ohtu sattuda inimeste elu ja tervis. Väga rasked tagajärjed võivad olla ka intsidentidel, mis on suunatud andmete tervikluse vastu, näiteks riigile olulistes andmekogudes.

Küberohtudele altina paistavad üle maailma silma eelkõige tervishoiu-, energia-, finants- ja sidesektor.

6. Analüüsitud stsenaariumid	**Riskiklass**
Elektroonilise isikutuvasuse ja digiallkirjastamise teenuse katkemine	E3 (kõrge)
Riigi toimimiseks oluliste andmete tervikluse rikkumine	E3 (kõrge)
Ulatuslikke elektrikatkestusi põhjustav küberrünnak	D4 (kõrge)
Andmesideteenuse katkestused	D3 (oluline)

7. Hädaolukorraks laieneda võivad sündmuse stsenaariumid:

1. Elektroonilise isikutuvasuse ja digiallkirjastamise teenuse katkemine
2. Riigi toimimiseks oluliste andmete tervikluse rikkumine
3. Ulatuslikke elektrikatkestusi põhjustav küberrünnak
4. Andmesideteenuse katkestused

Riskianalüüsis käsitletud stsenaariumide tõenäosus on kõrge ja tagajärjed võivad olla väga rasked. Tõenäosust ja tagajärgede raskusastet tõstab asjaolu, et valdkond muutub ja areneb kiirelt, samuti kasvab infosüsteemidest sõltumise määr üha enam, mistõttu on tõenäoline, et taolised sündmused võivad aset leida järgneva 5 aasta jooksul.

8. Elanikkonnakaitse meetmed

Avalikkuse teavitamine ning juhiste andmine.

9. Riskikommunikatsiooni meetmed

Küberintsidendi hädaolukorra osas ei ole vajalik planeerida eraldi riskikommunikatsiooni meetmeid. Ennetava tegevusena ja valmisoleku suurendamiseks on vajalik tõsta erinevate sihtgruppide turbeteadlikkust. Selle saavutamiseks viib Riigi Infosüsteemi Amet läbi erinevaid tegevusi:

- perioodilised raportid ja ohuhinnangud (kuukokkuvõtted, aastaraportid);
- RIA blogi, kübervaldkonna uudiskiri ja meediaartiklid/-kampaaniad;
- turvateadlikkuse tõstmise koolitused, infopäevad ja seminarid erinevatele

sihtgruppidele; • küberhügieeni juurutamine riigiasutustes (DigiTest keskkond); • CERT-EE hoiatused ja teated; • info haavatavustest ja soovitused nende kõrvaldamiseks.
10. Muud meetmed: Puuduvad