RISKIANKEET

1. Riskianalüüsi koostanud juhtiv asutus

Riigi Infosüsteemi Amet

2. Riskianalüüsi kinnitamise kuupäev

06.01.2021

3. Viide riskianalüüsile

Riigi Infosüsteemi Ameti peadirektori 06.01.2021 käskkiri nr 1.1-2/21-002

Riskianalüüs on tunnistatud asutusesiseseks kasutamiseks vastavalt AvTS § 35 lg 1 p 3, 9, 10, 18[1]

4. Hädaolukorda põhjustada võiva sündmuste liigid

Arvestades hädaolukorra seaduses kirjeldatud hädaolukorra definitsiooni ja tuginedes Riigi Infosüsteemi Ameti (RIA) eksperthinnangule käsitletakse küberintsidendi riskianalüüsis ainult neid sündmusi, mis võivad areneda hädaolukorraks.
Kokku käsiteltakse riskianalüüsis viit erinevat stsenaariumit, mille valik põhineb eelkõige üleilmsetel sündmustel, mis näitavad küberintsidentide trendi vastavates valdkondades.

Sellisteks sündmusteks on:

1. **Elektroonilise isikutuvastamise ja digitaalse allkirjastamise (eID) teenuse katkemine (elutähtsa teenuse katkestus);**
2. **Riigi toimimiseks oluliste andmete tervikluse rikkumine;**
3. **Ulatuslikke elektrikatkestusi põhjustav küberrünnak (elutähtsa teenuse katkestus);**
4. **Andmesideteenuse katkestused (elutähtsa teenuse katkestus);**
5. **Ulatuslik teenusetõkestusrünnak (mistahes elutähtsa(t)e teenus(t)e või muu(de) olulis(t)e teenus(t)e katkestused).**

5. Ülevaade toimunud sündmustest

1. Elektroonilise isikutuvastamise ja digitaalse allkirjastamise (eID) teenuse katkemine (elutähtsa teenuse katkestus)

2017. aastal aset leidnud ID-kaardi turvariski kaasus kinnitas, et krüptohaavatavus võib selguda väga ootamatult ning kaasa tuua märkimisväärsed tagajärjed. Intsidendiga kaasnevad mõjud on väga laiaulatuslikud ning puudutavad kogu riiki ja selle toimimist, tagajärjed ulatuksid ka väljapoole Eestit. Selleks, et tagada jätkusuutliku eID lahenduste ja turvalise andmevahetuskanali pakkumist, tasub mõelda nende toimimiseks kriitiliste teenuste dubleerimisele.

2. Riigi toimimiseks oluliste andmete tervikluse rikkumine

Eestis ei ole teadaolevalt toimunud laiaulatuslikke või sihitud ründeid, mis oleksid põhjustanud riigi toimimiseks oluliste andmete tervikluse rikkumist või olulist andmete tervikluse kadu riigile tähtsates süsteemides ja andmekogudes. Seevastu suuremate

tagajärgedeta lihtsamaid terviklusintsidente esineb sageli.
Motivatsioon digitaalse taristu usaldusväärsust õõnestada võib olla eeskätt vaenulike välisriikide eriteenistustel ja organiseeritud kuritegelikel rühmitustel, eesmärgiga kahjustada mainet, mõjutada otsustusprotsesse, kahjustada avalikku usaldust riigi toimimise suhtes või saavutada suurt majanduslikku kasu.

3. Ulatuslikke elektrikatkestusi põhjustav küberrünnak (elutähtsa teenuse katkestus)
Viimaste aastate jooksul on tihenenud rünnakud elutähtsat teenust osutavate ettevõtete ja nende teenuste vastu. Nendest teenustest ja protsessidest sõltub omakorda kogu tänapäeva ühiskonna harjumuspärane toimimine. Enim kõneainet on andnud pahavara Stuxnet ning rünnakud Ukraina elektrijaamade vastu.

4. Andmesideteenuse katkestused (elutähtsa teenuse katkestus)
Eestis ei ole toimunud laiaulatuslikku andmesidekatkestust, mis oleks põhjustanud hädaolukorra. Samas ühel teenusepakkujal on lühemaid teenusekatkestusi olnud korduvalt.

5. Ulatuslik teenusetõkestusrünnak (mistahes elutähtsa(t)e teenus(t)e või muu(de) olulis(t)e teenus(t)e katkestused)
Maailmas üldiselt näib teenusetõkestusrünnete trend 2020 aastal olevat tõusuteel nii arvuliselt kui ka oma mõju poolest. Arengud tehnoloogias, andmete majutamine pilves ja asjade internet loovad samuti soodsad tingimused uute rünnete teostamiseks.

6. Analüüsitud stsenaariumid

6.1.1. Krüptoalgoritmide rakendamine

Tugeva elektroonilise identiteedi tagamine toob järjest kiiremini arenevas ja muutuvas kübermaailmas kaasa suuri väljakutseid ning on muutumas üha keerulisemaks.

Kui krüptoalgoritmis või selle tehnilises juurutuses ilmneb turvaprobleem, võib see viia uute lahenduste välja töötamiseni. Olenevalt probleemi keerukusest võib tegemist olla aeganõudva protsessiga ning tuua endaga kaasa märkimisväärseid kulutusi.

Ootamatu sertifikaatide peatamine/sulgemine enne nende kehtivusaja lõppu mõjutab nende suure arvu tõttu nii riigi kui ka erasektori pakutavate e-teenuste kasutatavust ning toob kaasa mainekahju Eesti e-riigile.

6.1.2. Stsenaariumi riskiklass: **KÕRGE** (tõenäosus: suur, tagajärjed väga rasked)	6.1.3. Stsenaarium võib laieneda hädaolukorraks *(märkida sobiv)* **JAH** / EI

6.2.1. E-riigi toimimiseks kriitilise teenuse tõrked

E-riigi toimimiseks kriitilise teenuse tõrgete tõttu pole võimalik kasutada X-tee andmevahetuskihti ega ühtegi eID teenust (sh Mobiil-ID, ID-kaart, Smart-ID) minimaalselt **6-12 kuud** (sõltuvalt võimalikust lahendusest). Stsenaariumi tagajärjel puudub elektrooniline ligipääs teenustele ja dokumentidele, puudub võimalus kiiresti digitaalallkirjastada vajalikke dokumente, X-tee päringud ei tööta ning üleminek alternatiividele nõuab märkimisväärset ajakulu ja füüsilist kohalolekut. Halbade asjaolude kokkulangemisel võivad tagajärjed tuua kaasa ohu inimeste elule ja tervisele.

6.2.2 Stsenaariumi riskiklass: **KÕRGE** (tõenäosus: suur, tagajärjed väga rasked)	6.2.3. Stsenaarium võib laieneda hädaolukorraks *(märkida sobiv)* **JAH** / EI
6.3.1. Tervikluse intsident riigi toimimiseks olulises infosüsteemis Riigi jaoks olulistes infosüsteemides olevate andmete manipuleerimise, elektrooniliste andmete kadu ja tervikluse rikkumise tagajärjena võib riigi toimimine destabiliseeruda ning riigi otsused põhineda valeandmetel. Häired infosüsteemides tekitaksid oluliste teenuste katkemise. Tervikluse intsidendid on raskesti tuvastatavad, sest nende tuvastamine toimub pärast andmete reaalset muutmist, mistõttu sõltuvalt intsidendist on tegelikku aja- ja rahakulu raske prognoosida. Samuti seatakse kahtluse alla varasemate otsuste pädevus, mis on pannud Eesti sõltuma digilahendustest.	
6.3.2. Stsenaariumi riskiklass: **VÄGA KÕRGE** (tõenäosus: väga suur, tagajärjed väga rasked)	6.3.3. Stsenaarium võib laieneda hädaolukorraks *(märkida sobiv)* **JAH** / EI
6.4.1. Küberrünnak elektrisektori vastu Küberrünnak elektrisektori vastu, mis põhjustab talvisel ajal 7 päeva vältel ulatuslikke elektrikatkestusi. Katkestuste tulemusena tekivad häired teiste elutähtsate teenuste pakkumises ning tuhanded inimesed jäävad lühiajaliselt miinuskraadides hakkama saama ilma elektri, joogivee ja kütteta.	
6.4.2. Stsenaariumi riskiklass: **KÕRGE** (tõenäosus: suur, tagajärjed väga rasked)	6.4.3. Stsenaarium võib laieneda hädaolukorraks *(märkida sobiv)* **JAH** / EI
6.5.1. Küberrünnak andmesideteenuse pakkujate vastu Stsenaariumi tagajärjed on väga rasked ning mõjutavad kogu riiki ja selle toimimist. Suure ulatusega ning pikaaegne side katkemine vallandab omakorda muude (elutähtsate) teenuste katkemise ahelreaktsiooni, mille tagajärjel võib tekkida otsene oht inimeste elule ja tervisele, märkimisväärsed häired riigikorralduses ning suured varalised kahjud.	
6.5.2. Stsenaariumi riskiklass: **KÕRGE** (tõenäosus: suur, tagajärjed väga rasked)	6.5.3. Stsenaarium võib laieneda hädaolukorraks *(märkida sobiv)* **JAH** / EI
6.6.1. Ulatuslik teenusetõkestusrünnak Stsenaariumi tagajärjed on rasked ning mõjutavad kogu e-riiki ja selle toimimist. Ulatuslik teenusetõkestusrünne mitte ei halva ainult küberruumi, vaid toob kaasa ka seadme ja tulemüüri rikkeid, mis võivad omakorda häirida elutähtsate teenuste tööd. Ulatuslike teenuste katkestuse puhul võib tekkida otsene oht inimeste elule ja tervisele, kuna abivajajad ei pruugi saada ühendust Häirekeskusega või ravimeid digiretseptiga. Lisaks toob stsenaarium kaasa olulised majanduslikud kahjud, e-riigi mainekahju ning tekitab ühiskonnas suure ärevuse.	
6.6.2. Stsenaariumi riskiklass: **KÕRGE** (tõenäosus: väga suur, tagajärjed rasked)	6.6.3. Stsenaarium võib laieneda hädaolukorraks *(märkida sobiv)* **JAH** / EI
7. Käitumisjuhised ja sõnumid avalikkusele **Mida saab asutus/ettevõte/töötaja ise ära teha, et sellist olukorda ennetada:** • Kaardistada oma tehnoloogilise süsteemi komponendid, nendega seotud riskid, koostööpartnerid ning mõjutatud osapooled, rakendada vastavaid turvameetmeid.	

- Tagada süsteemi komponentide (riistvara, tarkvara, rakendused, teegid, turvaserverid jne) turvalisust ning paigaldada neile õigeaegselt versiooniuuendused. Eraldada muust võrgust need süsteemi komponendid, mis on kergemini rünnatavad.
- Kasutada sissetungi tõkestamise ja avastamise seadmeid
- Salvestada ja analüüsida oma võrguliiklust.
- Veenduda, et rakenduse ja turvaserveri vaheline suhtlus käib üle HTTPS kanali.
- Veenduda, et kasutatava turvaserveri pordid ei ole välisvõrgust ligipääsetavad, ilma täiendava kontrollita.
- Kasutada krüpteeritud andmevahetust ning mitme tasemelist autentimist.

Mida saab asutus/ettevõte/töötaja ise ära teha, et sellist olukorda ennetada:

- Valmistada ette plaani, et küberintsident ei halvaks pakutavate teenuste kättesaadavust ning harjutada see läbi.
- Planeerida regulaarsed auditid.
- Harida ennast küberhügieeni teemadel (Näiteks tutvuda RIA veebis ennetuste ja nõuannetega, kasutada Digitest platvormi, tutvuda IT-vaatlik kampaaniaga jne)
- Lisada ennast valdkonna infolisti (turvajuhid, administraatorid jne), kust jagatakse asja- ja ajakohast infot valdkonna arengute kohta.

Mida saab asutus/ettevõte/töötaja ise ära teha, kui selline olukord on juba tekkinud:

- Takistada küberintsidendi levikut.
- Teavitada olulisest intsidendist CERT-EE-d ning mõjutatud osapooli/partnereid.

8. Avalikkuse teavitamise kanalid

Käitumisjuhend avalikkusele hädaolukorraks ennetamisel/valmistumisel

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 (Ole IT-vaatlik!);

• turvateadlikkuse tõstmise koolitused, infopäevad ja seminarid erinevatele sihtgruppidele;

• küberhügieeni juurutamine riigiasutustes (DigiTest keskkond);

• CERT-EE hoiatused ja teated;

• info haavatavustest ja soovitused nende kõrvaldamiseks.

RIA avalik veebileht:

https://www.ria.ee/

Ole valmis! Küberrünnak või küberintsident:

https://www.olevalmis.ee/et/juhis/kueberruennak-voi-kueberintsident

Täiendav info CERT-EE tegevuste kohta:
https://www.ria.ee/et/kuberturvalisus/cert-ee.html

Täiendav RIA juhendmaterjal:
https://www.ria.ee/et/ametist/juhendid.html#riigi-infosusteem

Täiendav informatsioon kriisihalduse kohta:
https://www.ria.ee/et/kuberturvalisus/kriisihaldus.html

Täiendav informatsioon uuringute ja analüüside kohta:
https://www.ria.ee/et/ametist/uuringud-analuusid-ulevaated.html

Lisainfo eID arengute kohta:
https://www.id.ee/id-abikeskus/

Täiendav informatsioon eID teenuste kohta:
https://www.ria.ee/et/riigi-infosusteem/elektrooniline-identiteet-eid.html

eID kriisi korral on võimalik täiendavat lisainfot ja abi saada infotelefonidel:
ID abitelefon (tööpäeviti 8:00 – 19:00) (+372) 666 8888
Sertifikaatide peatamine (ööpäevaringne) 1777 ja (+372) 677 3377
Smart-ID klienditugi (ööpäevaringne) (+372) 715 1606

Lisainfo X-tee andmevahetuskanali kohta:
https://www.ria.ee/et/riigi-infosusteem/andmevahetuskiht-x-tee.html

X-tee abikeskus:
https://abi.ria.ee/xtee/et