# Väikese riskiklassiga ohud

Kristjan Krips

# Metoodika

- Üldise arhitektuuri, andmevoogude ja osaliste modelleerimine ehk ründepinna kaardistamine.
- Ohukategooriate kokkuleppimine.
- Riskianalüüsi metoodika kokkuleppimine.
- Hindamist vajavate komponentide ja ohtude jagamine komisjoniliikmete vahel.
- Ohukirjelduste ülevaatamine ja ühine hindamine.

# Riskiklass

- Riskiklassi väärtus on võrdne mõju (1-5) ja võimalikkuse (1-5) korrutisega.
- Küberturvalisuse komisjonis lepiti kokku neli risiklassi kirjeldust: väike, keskmine, suur, väga suur.
- **Väike (6-10, võetakse teadmiseks)**: Talutav risk. Riski teadvustatakse, kuid selle edasiseks vähendamiseks ei pruugita rakendada täiendavaid meetmeid. Tuleb kaaluda vajadust rakendada riski ennetavaid ja/või tagajärgi leevendavaid turvameetmeid ning hinnata, kas meetmete rakendamine on kasulikum kui riski aktsepteerimine.

# Ohusündmuste kategoriseerimine

- Kategoriseerisime ohusündmused nelja kategooriasse:
  - e-hääletamise ohud
  - m-hääletamise ohud
  - paberhääletamise ohud
  - üldohud

# Väike riskiklass: e-hääletamise ohud

- audiitor kasutab mitteautentset töötlemisrakendust / ei kontrolli töötlemisrakenduse autentsust ja tulemusena saab häälte töötlemise rakendus pahandust teha (hääli muuta, kustutada)
- juhendmaterjalide kompromiteerimine
- kogumisteenusele ja valijarakenduse ehitusprotsessile juurde pääsev ohuagent üritab takistada osade häälte vastuvõtmist
- kogumisteenusele ligi pääsev ohuagent üritab hääli pärast vastuvõtmist kustutada

# Väike riskiklass: e-hääletamise ohud

- kogumisteenusele ligi pääsev ohuagent üritab hääli muuta
- kompromiteeritud teenuse kaudu õngitsemine
- koodist leitakse uus probleem
- ohuagent peatab osade valijate ID-kaardi/mobiil-ID sertifikaadid
- rakenduse arendaja on kompromiteeritud
- sisulevivõrgu kaudu tekkiv terviklusrisk

# Väike riskiklass: m-hääletamise ohud

- kahjurvara tuvastab kas valija hakkab häält verifitseerima
- hääle kontrollimine ebausaldusvääse seadmega
- osa Apple App Store’i / Google Play Store’i sisulevivõrgust võib olla kolmandate riikide kontrolli all
- kahjurvara levitamine läbi m-valijarakenduse
- valimiste korraldaja ei testi m-hääletamise rakendust Androidi/iOS beetaversioonidel

# Väike riskiklass: paberhääletamise ohud

- kandidaatide nimekirja võltsimine hääletuskabiinis
- karusellhääletamine
- sedelite massiline hävitamine
- valija lekitab tahtlikult oma hääle
- valimiskabiini paigaldatakse jälgimisseadmed
- valimiskasti füüsiline ründamine

# Väike riskiklass: üldohud

- süvavõltsingute (*deep fake*) kampaania
- rahvastikuregistrisse lisatakse virtuaalseid kodanikke, kellele ei vasta füüsilist isikut
- siseriiklike internetimagistraalide katkemine
- valimiste korraldaja ei kommunikeeri auditite tulemusi

# Tänan!