Kriitilise informatsiooni infrastruktuuri (KII) kaitse simuleerimine Küberharjutusväljal

Kaitseministeerium

Märts 2018

Mis on Küberharjutusväli?

- Küberharjutusväli on riist- ja tarkvaraline keskkond, mis pakub meetodeid ja tehnoloogiat küberkaitse alase väljaõppe parandamiseks.
- Küberharjutusväli võimaldab optimeerida personali väljaõpet ja selle kulutusi, võimaldades kollektiivseid küberkaitseharjutusi.
- Küberharjutusväli võimaldab väljaõpet teha eraldiseisvas keskkonnas, mis ei mõjuta toodangusüsteeme.
- Küberharjutusväljal saab kasutada erinevaid stsenaariume küberrünnete läbiviimiseks, mida avalikes pilveteenustes ei saa teha või tuleb kasutada täiendavaid turvameetmeid.

Kaitseväe Küberharjutusväli

- Kasutusel alates 2012, alates 2013. aastast ka NATO Cyber Range
- Eesmärk – küberväljaõppe (kursused ja õppused) toetamine, tehniliste lahenduste testimine, valideerimine, eksperimenteerimine
- Opereerib Kaitsevägi, sisu toodavad erinevad osapooled
- Kasutajad - NATO Küberkaitsekoostöö Keskus, NATO väejuhatused, erinevad riiklikud partnerid jms
- Koosneb valdavalt *commercial-off-the-self* riist- ja tarkvarast, mida täiendavad erilahendused
- Toetab valdavalt tavapäraste IKT-võrkude simuleerimist

Erilahendused

- Lahendused, mida tavapäraste riist- ja tarkvaralahendustega pole reeglina võimalik simuleerida:
  - Tööstussüsteemid (Industrial Control Systems - ICS)
  - Värkvõrk (Internet of Things - IoT)
  - Industry 4.0
  - Autonoomsed sõidukid
  - Meditsiiniseadmed
  - Militaarsüsteemid
  - jne

Kriitilise informatsiooni infrastruktuur

- Elutähtis ehk kriitiline infrastruktuur on vara, süsteem või nende osa, mis on hädavajalik eluliselt tähtsate ühiskondlike toimingute toimimiseks. Näiteks tervishoiu, turvalisuse, julgeoleku, inimeste majandusliku ja sotsiaalse heaolu toimimiseks. See on infrastruktuur, mille kahjustada saamine või hävimine mõjutaks oluliselt riiki.
- Hädaolukorra seadusest § 36 lg 1:
  1) elektriga varustamine;
  7) andmesideteenus;

Uurimisvaldkonnad projekti raames

- Elektrisüsteemid (kuni 20kV)
  - Elektritootjad
  - Alajaamad / ülekanne
  - Elektritarbijad
- Mobiilsidesüsteemid (4G ja võimalikud edasiarendused)
  - Kesksed komponendid mobiilsidesüsteemi toimimiseks
  - Füüsilised baasjaama komponendid
  - Klientseadmed
  - Klientseadmete rakendused, mis toetavad uuringu eesmärke
  - Muud komponendid (SIM-kaardid jms)
- Tegemist ei ole kaitsevaldkonna projektiga

Eesmärk

- Analüüsida nimetatud KII valdkondades tehtud olulisemaid uurimis-, simuleerimis- jmt teadusprojekte Eestis ning Euroopas ning erinevad andmeallikad, mida on võimalik projekti realiseerimiseks kasutada.
- Töötada välja metoodika ja lahendused reaalsete KII keskkondade (hõlmab nii kontorivõrku- kui ka spetsiaalsüsteeme) simuleerimiseks Küberharjutusväljal.
- Uurida ja võtta kasutusele olemasolevad tehnoloogiad turvalise andmevahetuse seadistamiseks spetsiaalsüsteemide ja/või kontorivõrgu vahel.
- Uurida ja võtta kasutusele olemasolevad tehnoloogiad spetsiaalsüsteemide andmete (näiteks komponendi konfiguratsiooni või sellesse sisestatud andmekogumi) tervikluse kaitseks.

Oodatavad tulemused

- Metoodika KII valdkondadega seotud kasutusjuhtude kirjeldamiseks, hindamiseks ja süsteemide vaheliste sõltuvuste kirjeldamiseks.
- Üks turvalist andmevahetust pakkuv tehnoloogia, kirjeldatud selle kasutus spetsiaalsüsteemide andmete vahetamiseks ning loodud näidisrakendus Küberharjutusväljal.
- Üks andmete tervikluse kontrolli tagav tehnoloogia, kirjeldatud selle kasutus spetsiaalsüsteemide andmete tervikluse tagamiseks ning loodud näidisrakendus Küberharjutusväljal.
- Minilinn, millel on võimalik demonstreerida KII valdkonnast tulenevaid mõjusid elukeskkonnale ja valdkondade vahelisi ristsõltuvusi. Minilinn toimib *proof-of-concept*'ina ning peab olema laiendatav ka täiendavate moodulitega (näiteks raudteevõrguga).

Projekti ajakava

- Planeeritud pikkuseks ca 24 kuud
- I etapp - uurimisküsimuste ja skoobi täpsem määratlemine, baasuuringu läbiviimine, sh tehnilise lahenduse lähteülesande väljatöötamine
- II etapp ja III etapp (paralleelselt) – elektri- ja mobiilsidesüsteemi lahenduste implementeerimine
- IV etapp - dokumentatsiooni koostamine, lõpparuande koostamine, tulemuste esitamine

Eeldatavad kompetentsid

- Pakkujal peab projektimeeskonnas olema vähemalt üks isik, kes on viimasel viiel aastal avaldanud küberkaitse alaseid publikatsioone.
- Pakkujal peab projektimeeskonnas olema vähemalt üks isik, kes omab riigisaladusele juurdepääsuluba vähemalt tasemel PIIRATUD või samaväärset salastatud välisteabe luba (näiteks NATO PIIRATUD).
- Konsortsiumis on vähemalt üks ettevõte või ekspert, kes on tegev elektrisüsteemide valdkonnas elektriettevõtjana või vastavate lahenduste pakkujana.
- Konsortsiumis on vähemalt üks ettevõte või ekspert, kes on tegev mobiilsidesüsteemide valdkonnas sideettevõtjana või vastavate lahenduste pakkujana.