EUROOPPALAINEN HYBRIDIUHKIEN TORJUNNAN OSAAMISKESKUS
HELSINKI

LAUSUNTO

27.9.2018

Valtiovarainministeriö

Lausuntopyyntö VM115:00/2016 (16.8.2018)

POIKKEUSOLOIHIN VARAUTUMISTA RAHOITUSALALLA KOSKEVAN LAINSÄÄDÄNNÖN TARKISTAMINEN

Hybridiuhkilla tarkoitetaan moninaista tahallista ja laitonta vaikuttamista jonkin yhteiskunnan eri rakennelmiin ja järjestelmiin. Hybridiuhkia aiheuttavat valtiolliset ja ei-valtiolliset toimijat.

Hybriuhkista tehtyjen analyysien mukaan tällainen hyökkäys voi olla osa laajempaa poliittista ja sotilaallista toimintakokonaisuutta. On siis varauduttava sellaisiinkin tapahtumiin, joita ei voi ennustaa normaalin liiketoiminnan ja siihen kohdistuvan tähän asti tunnistetun kyber- ja muun rikollisuuden perusteella. Hybridioperaatiolla voidaan pelkästään häirintävaikutuksen aiheuttamiseksi pyrkiä lamauttamaan maksuliikenne tai hävittämään varallisuuden siirtoja ja varallisuuden hallintaa koskevia tietoja. Tähän voi liittyä myös taloudellisia spekulaatioita.

Tähän asti tunnetuista kyberiskuista vahvin on NotPetya-haittaohjelma, joka kesäkuussa 2017 levisi laajasti Ukrainassa ja siltä myös useisiin monikansallisiin yrityksiin. Taloudelliset tappiot ovat Yhdysvaltain hallinnon väittämän mukaan kokonaisuutena 10mrd dollarin luokkaa. Tämä tapahtuma - niin kuin siitä julkisuudessa on raportoitu – osoittaa, että moderneimpienkin liikeyritysten tietojärjestelmiin voidaan hyökätä yllättäen ja voimakkaasti.

Yllä kuvattuun uhkaan varautumisen kannalta olisi tarpeellista synnyttää sellaiset järjestelyt, joilla riittävän ajantasaiset (mutta ei välttämättä reaaliaikaiset) tiedot voidaan aina palauttaa laajan tiedostoja tuhonneen hyökkäyksen jälkeen. Lisäksi olisi tarpeen huolehtia väestön päivittäisen toimeentulon mahdollistavan maksuvalmiuden ylläpitämisestä tilanteessa, jossa tietoverkoissa ja sähköverkossa on laajoja ja pidempään kestäviä häiriöitä.

Haavoittuvuudet ja Resilienssi
-verkoston johtaja

Jukka Savolainen