|  |  |  |  |
| --- | --- | --- | --- |
| **VAHVUUDET**  **Positiivisten tekijöiden vaikutus kyberluottamusta lisääviin toimenpiteisiin** | | | **HEIKKOUDET**  **Negatiivisten tekijöiden vaikutus kyberluottamusta lisääviin toimenpiteisiin** |
| S I S Ä I S E T | **Johtaminen:** | **Johtaminen:** | |
| * kyberturvallisuus ja tietoturvallisuus huomioitu strategisena tavoitteena * tärkeimmät uhat tunnistettu, * riskiperusteinen, * toimenpiteitä priorisoitu | * vaativimmat uhkakuvat tunnistamatta * toiminta reagoivaa * henkilöstön roolitus usein haastavaa, | |
| **Tilannekuva:** | **Tilannekuva:** | |
| - uhkatiedot saadaan usein toiminta- verkostosta ja kumppaneilta suoraan | * yleistilanne muodostettava hajallaan olevista tiedoista * toimintaverkoston tilannekuvan muodostaminen   vaikeaa | |
| **Henkilöstön osaaminen:** | **Henkilöstön osaaminen:** | |
| * IT-henkilöstöllä hyvää osaamista * muulle henkilöstölle annetaan usein koulutusta verkossa | * koko henkilöstön kouluttaminen haastavaa * osaaminen harvojen käsissä (resursointi) * IT - kokonaisuuden ymmärtäminen | |
| **Tuotteet ja palvelut:** | **Tuotteet ja palvelut:** | |
| * parhaat tuotteet käytössä * palveluissa hyvä osaaminen * ulkoistettuna ostopalveluna, osin hajautettu riskiperusteisesti * työasemat usein omana palveluna, mikä sopii ”tavanomaisiin” uhkiin | * kumppanuusverkoston toiminnan auditointi haastavaa * puutteellinen näkymä palvelujen suojaukseen (mm. pilvipalvelut) * kattavan tunnistautumisen puute | |
| **Sidosryhmät:** |  | |
| - ulkoistuksissa parhaat kumppanit | **Sidosryhmät:** | |
| **Asiantuntijapalvelut:** | - osalla toimialoista toimialayhteistyö- mahdollisuuden puute | |
| * erilaiset auditointikäytänteet käytössä * ongelmatilanteiden selvittämisessä käytetään alan asiantuntijoita | **Asiantuntijapalvelut:**  - auditoinnin kattavuus läpi koko toiminnan ja ohjelmistojen toimintaan/palveluun  puutteellista | |
| - parhaat käytänteet käytössä | koulutuspalvelujen saatavuudessa haasteita | |
| **Jatkuvuuden varmistaminen:** |  | |
| * harjoitustoimintaa * varautumissuunnitelmia laadittu |  | |
| ul | **MAHDOLLISUUDET**  **Lista mahdollisuuksista, jotka lisäävät kyberluottamusta** | **UHKAT**  **Lista uhkatekijöistä, jotka vaikuttavat kyberluottamukseen** | |
| U  L  K  O  I  S  E  T | **Edistyksellisen tekniikan hankinta:**   * mahdollisuus investoida uuteen tekniikkaan   **Uudet yhteistyötahot:**   * + nykyistä laajemman toimialayhteistyön mahdollisuudet   **Uudet kehitysmahdollisuudet:**   * + toimintaedellytykset   + koulutuksen jatkokehittäminen   + benchmarking-toiminta   + auditointitoiminnan kehittäminen   + hallittu regulaatio (toimintojen harmonisointi) | **Toimintaympäristön analysointi:**   * tuntemattomat uhkatekijät ja tietomurrot * uudet liiketoimintamallit; edellyttävät uusien tekniikoiden käyttöönottoa (esim. IOT, robotiikka), joiden mukanaan tuomaa uhkakuvaa ei tunneta riittävästi   **Kyberuhkien analysointi:**   * haasteena teollisuusvakoilu * pysyykö ohjelmistokehitys uhkien mukana; vanhentunutta suojaustekniikka käytössä * henkilöstöriskit, sisäpiiriläiset * avainhenkilöstöön kohdistuvat uhat * kyberuhat keskittyneisiin palveluihin   **Toimintaverkoston analysointi:**   * ei näkymää verkostoon ja sen riippuvuussuhteisiin * resurssikapeikot laajojen häiriöiden tilanteessa | |