Kertomusluonnoksesta annetut lausunnot

Kybersuojauksen järjestäminen
(16/2017)
185/54/2016

Liikenne- ja viestintäministeriö, 10.8.2017.
Oikeusministeriö, 15.8.2017.
Valtioneuvoston kanslia, 15.8.2017.
Valtakunnanvoudinvirasto, 17.8.2017.
Valtion tieto- ja viestintätekniikkakeskus Valtori, 17.8.2017.
Oikeusrekisterikeskus, 21.8.2017.
Turvallisuuskomitea, 21.8.2017.
Valtiovarainministeriö, 21.8.2017.
Viestintävirasto, 21.8.2017.
Väestörekisterikeskus, 21.8.2017.
Liikenteen turvallisuusvirasto Trafi, 30.8.2017.

Konserniohjausosasto / Hallintoyksikkö

10.8.2017

Asianumero
LVM/1292/02/2017

Valtiontalouden tarkastusvirasto
tuloksellisuustarkastus@vtv.fi

Lausuntopyyntö 22.6.2017 185/54/2016

Liikenne- ja viestintäministeriön lausunto kybersuojauksen järjestämistä käsittelevään tarkastuskertomusluonnokseen

Valtiontalouden tarkastusvirasto on pyytänyt liikenne- ja viestintäministeriön lausuntoa tarkastuskertomusluonnoksesta ”Kybersuojauksen järjestäminen”. Lausuntopyynnön tarkoituksena on erityisesti varmistaa, että kertomukseen ei sisälly asia- tai tulkintavirheitä, joilla olisi vaikutusta tarkastuksen kannanottoihin, sekä kuulla lausunnonantajien näkemys tarkastusviraston alustavista kannanotoista.

Liikenne- ja viestintäministeriö esittää, että tarkastuskertomusta viimeistelтäessä huomioitaisiin seuraavat havainnot:

Tarkastuskertomusluonnoksessa suositellaan, että valtiovarainministeriö määrittelisi laajavaikutteisen kyberloukkaustilanteen operatiivisen johtamisen prosessin.

Liikenne- ja viestintäministeriön aikaisempien esitysten ja näkemyksen mukaan kyberturvallisuuden johtamisessa tulisi noudattaa valtioneuvoston normaalia johtamisjärjestelmää, joka on kuvattu muun muassa valtioneuvoston kokonaisturvallisuutta koskevassa periaatepäätöksessä. Kyberturvallisuusstrategian mukaan kyberturvallisuutta ei ole tarkoitettu oikeudelliseksi käsitteeksi, joka perustaisi uusia toimivaltuuksia viranomaisille tai muille toimielimille. Asiaa on käsitelty ministeriöiden välillä kyberturvallisuusstrategian toimeenpano-ohjelman valmistelun yhteydessä ja lisäksi kyberturvallisuuden johtamisesta ollaan aloittamassa VNTEAS-selvitys.

Kohdassa 2.4 kybersuojausta kehitetään enemmän paikoitellen kuin kokonaisuutena, todetaan verkko- ja tietoturvadirektiiviä koskevassa kirjauksessa olevan epäselvää, miten yhdenmukaisella tavalla NIS-direktiivi Suomessa implementoidaan, jos implementoinnin lähtökohta on toimialalähtöisyys. Tarkastusviraston tulkinta ei vaikuta aivan oikealta, sillä täytäntöönpanon toimialalähtöisyyden tavoitteena on ottaa eri toimialoja koskevat voimassa olevan lainsäädännön velvoitteet parhaalla mahdollisella tavalla huomioon ja mahdollistaa toiminnan harjoittajien ottaa tietoturvariskienhallinta kokonaisvaltaisesti osaksi normaalia turvallisuusriskienhallintaa ja näin osaksi yrityksen jokapäiväisiä normaaleja toimintatapoja.

Kohdassa 3.1 käytännön menettelyissä kybersuojauksen tilannekuvan luomiseksi on puutteita, käsitellään julkishallintoa 28.5.2018 alkaen velvoit-

Liikenne- ja viestintäministeriö
Käyntiosoite
Eteläesplanadi 16
(kirjaamo)
Helsinki
Postiosoite
PL 31
00023 Valtioneuvosto
Puhelin
029516001
www.lvm.fi
etunimi.sukunimi@lvm.fi
kirjaamo@lvm.fi

tavaa EU:n yleistä tietosuoja-asetusta. Tarkastuskertomusluonnoksen mukaan asetus velvoittaisi ilmoittamaan henkilötietojen kohdistuvista kyberloukkauksista Kyberturvallisuuskeskukselle ja tekemään kyberloukkauksista rikosilmoituksen poliisille. Liikenne- ja viestintäministeriö toteaa, että asetus ei velvoita tekemään ilmoitusta Kyberturvallisuuskeskukselle vaan kansalliselle valvontaviranomaiselle, joka määritellään oikeusministeriössä parhaillaan käynnissä olevassa lainsäädäntöhankkeessa.

Lisäksi käsityksemme mukaan EU:n yleinen tietosuoja-asetus ei velvoita tekemään henkilötietojen loukkauksista rikosilmoitusta poliisille.

Juhapekka Ristola
Osastopäällikkö, ylijohtaja

Jussi Luomajärvi
Hallintojohtaja

Liikenne- ja viestintäministeriö
Käyntiosoite
Eteläesplanadi 16
(kirjaamo)
Helsinki
Postiosoite
PL 31
00023 Valtioneuvosto
Puhelin
029516001
www.lvm.fi
etunimi.sukunimi@lvm.fi
kirjaamo@lvm.fi

OIKEUSMINISTERIÖ

LAUSUNTO

OM 8/05/2016
OM 7/05/2016

15.8.2017

tuloksellisuustarkastus@vtv.fi

viite: Lausuntopyyntönne dnro 340/54/2015 ja dnro 185/54/2016

OIKEUSMINISTERIÖN LAUSUNTO TARKASTUSKERTOMUSLUONNOKSIINNE SÄHKÖISTEN PALVELUIDEN TOIMINTAVARMUUDEN OHJAUS JA KYBERSUOJAUKSEN JÄRJESTÄMINEN

Oikeusministeriöllä ei ole kommentoitavaa oikeusministeriötä ja sen hallinnonalan virastoja (Oikeusrekisterikeskus, Valtakunnanvoudinvirasto) koskeviin kohtiin toimintakertomusluonnoksissa.

Pienenä epätarkkuutena Sähköisten palveluiden toimintavarmuuden ohjausta koskevassa tarkastuskertomusluonnoksessa on sivulta 32 löytyvä maininta "Oikeusrekisterikeskus hankkii perustietotekniikkapalvelut Valtorilta", jonka voisi tarkentaa "Oikeusministeriö ja Oikeusrekisterikeskus hankkivat hallinnonalan perustietotekniikkapalvelut Valtorilta". Lisäksi sivulla 34 todetaan "Oikeusrekisterikeskus ja Valtakunnanvoudinvirasto laativat vuosittain toimialasidonnaisten ICT-palvelujen vuosisopimuksen." Tämän lisäksi voisi todeta, että "Oikeusministeriön tietohallintoyksikkö laatii vuosittain palvelusopimuksen Valtorin kanssa hallinnonalan toimialariippumattomien palveluiden tuottamisesta".

Tietohallintojohtaja Tarmo Maunu

Erityisasiantuntija Riitta Marttila

Käyntiosoite	Postiosoite	Puhelin	Faksi	Sähköpostiosoite
Eteläesplanadi 10 HELSINKI	PL 25 00023 VALTIONEUVOSTO	02951 6001	09 1606 7730	oikeusministerio@om.fi

VALTIONEUVOSTON KANSLIA
STATSRÅDETS KANSLI

Lausunto VNK/1868/01/2016

15.8.2017

Viite VNK/1868/01/2016 Lausuntopyyntö VTV:n tarkastuskertomusluonnoksesta; Kybersuojauksen järjestäminen

Asia **Lausunto VTV:n tarkastuskertomusluonnoksesta; Kybersuojauksen järjestäminen**

Valtioneuvoston kanslia esittää lausuntonaan tarkastuskertomusluonnoksesta seuraavaa.

Tarkastuskertomuksessa esitetyt näkemykset operatiivisen ohjauksen ja yhteisen tilannekuvan puutteesta, kybersuojauksen hajanaisuudesta ja rahoitusratkaisujen tarkoituksenmukaisuudesta ovat hyviä huomioita. Valtioneuvostokin piirissä kyseiset asiat ovat hajallaan: Valtori vastaa vajavaisin resurssein omien palveluidensa kybersuojauksesta, joista yksi tärkeimmistä on valtion yhteinen verkko ja valtioneuvoston kannalta myös valtioneuvoston verkko.

Kuten raportissa mainitaan, kybersuojauksen ammattiosaamisesta on niukkuutta. Siksi kybersuojauksen toteuttamisessa yhteistyö ja -toiminta ovat tärkeitä. Valtioneuvoston piirissäkin esim. ulkoasiainministeriöllä on pitkälle erilliset kybersuojausjärjestelyt ja huomattavasti enemmän resursseja kuin muulla valtioneuvostolla. Tämä siitä huolimatta, että ulkoasiainhallinnon kansainvälistä verkkoa hallinnoi Valtori valtioneuvoston kanslian ohjauksessa.

Kybersuojauksen keinoista raportti tunnistaa mm. tekniset suojauskeinot sekä peruskäyttäjien tietoisuuden ylläpitämisen. Näiden lisäksi raportissa voisi mainita keskeisistä hallinnollista suojauskeinoista ainakin palveluiden tehokkaan hallinnan ja operatiivisen henkilökunnan ajantasaisen ammattitaidon. Kummassakin näistä on nykytilanteessa parantamisen varaa.

Kuten raportissa mainitaan, kybersuojauksen tason määrittää tosiasiallisesti lähinnä määrärahojen riittävyys, ei niinkään nykyinen riskipositio. Tämä pätee nykytilanteessa moneen muuhunkin asiaan. Raporttiin olisi hyvä lisätä huomio, että riskienhallinnan määrätietoisempi käyttö vaatisi toimintojen ja niiden kriittisyyden ja tätä kautta myös tietoteknisten palveluiden kriittisyyden tarkempaa määrittelyä.

Valtionhallinnon vastuusuhteet ovat lainsäädännön tasolla monimutkaiset. Kuten raportissakin todetaan, päätöksenteko nopeaa reagointia vaativissa kyber-

Snellmaninkatu 1, Helsinki | PL 23, 00023 Valtioneuvosto | PUHELIN/TELEFON 0295 16001 (vaihde/växel) | FAKSI/FAX (09) 1602 2165 | kirjaamo@vnk.fi
Snellmansgatan 1, Helsingfors | PB 23, 00023 Statsrådet | | | registratorskontoret@vnk.fi

hyökkäyksissä on tuskin riittävän nopeaa. Tämän vuoksi valtionhallinnossa olisi tehtävä etukäteen päätökset ja toimintamallit siitä kuinka laajassa hyökkäystilanteessa toimitaan. Raportin viittaus valmiuslakiin ei ole relevantti, sillä kyseisen lain käyttöönotto vaatinee aikaa enemmän kuin kyberhyökkäyksen tehokkaaseen torjuntaan on mahdollista käyttää.

Toimintavarmojen digitaalisten prosessien ja palveluiden edellyttämää kybersuojauksen toteuttamista hankaloittaa Valtorin toiminnan perustuminen asiakasrahoitukseen. Tämä tekee muiden kuin tuotteistettujen palveluiden kehittämisestä hankalaa. Esimerkkinä tällaisista keskeisistä kokonaisuuksista voidaan mainita palvelunhallinnan yhdenmukaistaminen ja palveluiden kyberturvallisuuden kustannustehokas ylläpito ja kehittäminen. Valtorin palveluiden puutteellinen tietoturvavalvonta on osaltaan johtanut siihen, että jotkut virastot ovat hankkineet tai hankkimassa ulkopuolisilta palveluntarjoajilta omaa kyvykkyyttä tietoverkkojensa tietoturvavalvontaan ja kybertilannekuvan ylläpitoon. Tällöin menetetään palveluiden keskittämisen hyötyjä muun muassa osaamisen ja resurssien näkökulmasta. Tilanne voi olla myös lainsäädännöllisesti kyseenalainen liittyen Valtorin lainsäädännössä määriteltyihin yksinoikeustehtäviin.

Raportissa mainitaan, että Valtorin *"palvelujen määrän vuoksi tilannetieto ei ole ohjelmistoista ja ohjelmistoversioista ei ole reaaliaikainen"*. Tämä tulkinta on VNK:n mielestä puutteellinen. Tilannetieto ei ole reaaliaikainen lähinnä siksi, että tietoa ei pidetä yllä resurssien alimitoituksen ja kehittämisrahoituksen puuttumisen takia.

Raportin mukaan Valtorille virastoilta siirtyneet palvelut *"on tarkoitus lopettaa siirtymäkauden aikana ja siirtyä käyttämään TORI-palveluita"*. Tässä on syytä huomata, että siirtymäkaudelle ei ole asetettu määräaikaa. Lisäksi virastojen on itse hankittava rahoitus projekteihin, joilla siirrytään uusiin palveluihin ja ajetaan vanhat alas.

Yhteenvetona todettakoon, että tarkastuskertomusluonnos esittää pääosin hyvin kybersuojauksen nykytilan. Luonnos kuvaa riskienhallinnan käytäntöjen kirjavuuden sekä huolestuttavat puutteet mahdollisen kyberhyökkäyksen havainnointi- ja reagointikyvyssä. Myös Valtorin toimintaan ja rahoitukseen liittyvät kybersuojauksen kehittämistä rajoittavat haasteet on raportissa huomioitu.

Timo Lankinen
Alivaltiosihteeri

Petri Puhakainen
Neuvotteleva virkamies

Jakelu

Valtiontalouden tarkastusvirasto

Tiedoksi

VNK tietotoimiala

VALTAKUNNANVOUDINVIRASTO

17.8.2017

Lausunto asiassa
VTV Dnro
185/54/2016

Dnro VVV 388/331/17

Valtiontalouden tarkastusvirasto
tuloksellisuustarkastus@vtv.fi

Viite Lausuntopyyntö luonnoksesta tarkastuskertomukseksi kybersuojauksen järjestämiestä

ASIA Valtakunnanvoudinviraston lausunto

Lausunto Valtakunnanvoudinvirasto lausuu asiassa seuraavaa:

Lausuntopyynnön tarkoituksena on erityisesti varmistaa, että kertomukseen ei sisälly asia- tai tulkintavirheitä, joilla olisi vaikutusta tarkastuksen kannanottoihin, sekä kuulla näkemys tarkastusviraston alustavista kannanotoista.

Valtakunnanvoudinvirasto katsoo, että tarkastuskertomus on asia- ja tulkintasisällöltään oikean sisältöinen, eikä alustavissa kannanotoissa ole huomautettavaa.

Valtakunnanvouti Juhani Toukola

Johtava hallintovouti Veikko Minkkinen

Käyntiosoite	Postiosoite	Puhelin	Telekopio	Sähköpostiosoite
Ratapihantie 9 00520 HELSINKI	PL 330 20101 TURKU	029 56 65180	029 56 65159	vvv@oikeus.fi

Kommentit VTV:n lausuntopyyntöön tarkastuskertomusluonnoksista Kyberturvallisuuden järjestäminen ja Sähköisten palveluiden toimintavarmuuden ohjaus

Valtorin johtoryhmä ja tuloksellisuustarkastuksiin osallistuneet henkilöt ovat tutustuneet tarkastuskertomusluonnoksiin ja tehneet seuraavassa kuvatut kommentit ja huomiot. Kokonaisuutena Valtori pitää tarkastuskertomusluonnoksia oikeellisina, kattavina ja asianmukaisina.

1 Kybersuojauksen järjestäminen

Luonnoksen mukaan tarkastuksen tavoitteena oli

"*selvittää, onko valtionhallinnon kybersuojaus järjestetty mahdollisimman vaikuttavasti ja taloudellisesti tarkoituksenmukaisella tavalla.*"

Tarkastuskertomuksessa ei arvioida selkeästi asetettujen tavoitteiden toteutumista. Materiaalin perusteella olisi kenties perusteltua sanoa, että tarkastuksen mukaan valtionhallinnon kybersuojauksen vaikuttavuudessa on puutteita, jotka suurelta osin johtuvat kybersuojauksen toteuttamisen puutteellisesta ja epäselvästä rahoituksesta ja resursoinnista.

Tarkastusvirasto ei ehkä riittävän selkeästi kiteytä ja konkretisoi aineistosta selvästi esiin tulevaa kyberturvallisuuden johtamisen liittyvää talouden ongelmaa: ristiriita hyvän tahtotilan ja siihen pääsemisen liittyvien kulujen välillä. Kyberturvallisuuden hoidossa ollaan riippuvaisia rahoitusratkaisuista ja niistä johtuvista resursseista. Valtorin resurssit riippuvat suoraan asiakasvirastojen halusta käyttää ICT-määrärahojaan kyberturvallisuutta kehittävään työhön Valtorissa. Kyberturvallisuuden kehittäminen olisi syytä esittää sellaiseksi, että sen rahoitus ei ole riippuvainen eri asiakasvirastojen panostuksesta ja käytettävissä olevista määrärahoista.

Tarkennetut kommentit luonnoksen sisältöön:

- Kohta 3: ”*Valtori parantaa kybersuojauksen menettelyjen ja kyberloukkausten havainnoinnin toteutusta, arviointia ja kehittämistä*”

Tavoite on ilman muuta oikea, mutta nettobudjetoituna erityisvirastona Valtorin mahdollisuudet toimia rajoittuvat erillisrahoituksen tai palveluiden hinnankorotusten myötä tehtäviin toimenpiteisiin. Tämä on hyvä huomioida myös suosituksissa.

2 Sähköisten palveluiden toimintavarmuuden ohjaus

- Sivu 16: ” Ongelmana on se, että viime kädessä tietoturvallisuudesta vastaa aina varsinaisesta toiminnasta tai palvelusta vastuussa oleva taho.”

Tässä on hyvä tarkentaa, että tietoturvallisuuteen liittyvät vastuut voidaan jakaa kahteen erilliseen kokonaisuuteen: kokonaisvastuu ja toteutusvastuu. Toiminnan, palvelun tai tietojen omistajalla on aina kokonaisvastuu, eli ns. viime käden vastuu tietoturvallisuudesta, mukaan lukien kyseisten kohteiden turvallisuudelta edellytettävän vaatimustason määrittäminen. Tätä vastuuta ei koskaan voida ulkoistaa. Määritettyjen vaatimusten toteutusvastuu voidaan ulkoistaa, kuten tässä tapauksessa Valtorille.

Oikeusrekisterikeskus
PL 157, 13101 HÄMEENLINNA

21.8.2017 Dnro 164/00/2017

Valtiontalouden tarkastusvirasto
Pasi Korhonen
PL 1119
00101 HELSINKI

Viite:
VTV/Dnro 185/54/2016

LAUSUNTO TARKASTUSLUONNOKSEEN

Valtiontalouden tarkastusvirasto (VTV) on pyytänyt Oikeusrekisterikeskukselta (ORK) lausuntoa tarkastuskertomusluonnokseen Kybersuojauksen järjestämisestä (VTV/Dnro 185/54/2016).

ORK on arvioinut tarkastusluonnoksen ja esittää seuraavat huomiot ja kommentit tarkastusluonnokseen. Huomioiden ja kommenttien kohdalla sivunumero on PDF-dokumentin sivunumero.

Tarkastuskertomusluonnos Kybersuojauksen järjestäminen

Sivu 4 ”Keskittämisen myötä tarve yhtenäisempään ja kattavampaan riskienhallintaan on kasvanut.”

Erityisesti eri viranomaisten toiminnan edellyttämien kriittisten tietojärjestelmien verkottuessa on tarve yhtenäistää, sopia ja viestiä sovitusti merkittävistä riskeistä. Lisäksi kun jokin riski toteutuu, on havaittavissa selkeä puute ettei valtionhallinnon taikka laajemmin julkishallinnon viranomaisilla ole ilmoitusvelvollisuutta kyberloukkaustilanteissa (Viestintäviraston Kyberturvallisuuskeskukselle) jolloin muodostuu tilannetulkintaa useassa paikassa ja kokonaisuudesta muodostettava tilannekuva saattaa jäädä vajavaiseksi.

Oikeusrekisterikeskus
PL 157, 13101 HÄMEENLINNA

21.8.2017 Dnro 164/00/2017

Sivu 6. ”ICT:n organisoinnin muutoksissa pitäisi huomioida myös kybersuojaus”

Tähän havaintoon voisi lisätä myös näkökulman organisoinnin muutoksien vaikutuksista kybersuojauksen epäselvään vastuujakoon mm. tilannekuvan jakamiseen: yhteisissä palveluissa ja alustapalveluissa tulisi olla selvät vastuujaot sekä menettelyt kyberturvallisuuden tilanteen seurantaan, valvontaan ja tilanteiden viestintään, koska esim. Valtori ei voi vastata toimialasidonnaisten tietojärjestelmäpalveluiden sisälle tapahtumista eivätkä toimialasidonnaisten tietojärjestelmäpalveluiden omistajat ja rekisterinpitäjät voi puolestaan vastata Valtorin tuottamista palveluista.

Sivu 6. ” Valtiohallinnon organisaatioiden velvoittaminen ilmoitusten tekemiseen parantaisi tilannekuvan laatua, kuten myös keskitettyjen kyberloukkausten havainnointimenettelyjen kattavuuden lisääminen.”

Valtionhallinnon lisäksi myös laajemmin julkishallinnon pitäisi olla ko. ilmoitusvelvollisuuden piirissä, koska monet toiminnot ja prosessit edellyttävät myös mm. kuntaviranomaisten ja muiden toimijoiden riittävää yhteistyötä ja tiedonjakoa.

Sivu 13. ”Ministeriötasolla asiaa mutkistavat tilaaja-tuottaja-järjestelyt, joissa ministeriö hankkii valtioneuvoston hallintoyksikön välityksellä palvelun Valtorilta”

Lisäksi useat ministeriöt hankkivat palveluita oman hallinnonalansa toimialasidonnaisia tietojärjestelmäpalveluita palvelukeskuksilta, jotka puolestaan hankkivat osan palveluista Valtorilta.

Sivu 19. ” avainhenkilötä”

Kirjoitusvirhe avainhenkilöitä.

Sivu 19. ”kuten riittävästi resursoitua ympärivuorokautista varallaolotoimintaa (SecICT)”

SecICT-hankkeella oli eri tehtävä, voisi kirjata toisin, esim. … kuten riittävästi resursoidun valtionhallinnon ympärivuorokautisen tietoturvatoiminnan (SecICT-hankkeen) kehittämistä …

Oikeusrekisterikeskus
PL 157, 13101 HÄMEENLINNA

21.8.2017 Dnro 164/00/2017

Sivu 20. ”Palvelujen yhteen kokoaminen tuo riskin laajavaikutteisesta tuotantokatkoksesta”

Yhteen kokoaminen tuo mukanaan myös muitakin riskejä, esim. riskit tietomurroista ja -vuodoista yhden keskitetyn palvelutuottajan kautta.

Sivu 23. Kuvio 1.

Yhtenä toimijana voisi olla erikseen poikkihallinnollinen VIRT-toiminta, kuten mm. sivulla 25 mainitaankin.

toimialajohtaja Jari Saarela

kehittämispäällikkö Kimmo Janhunen

Viite:Valtiontalouden tarkastusviraston lausuntopyyntö 22.6.2017, Dnro 185/54/2016

Turvallisuuskomitean sihteeristön lausunto kybersuojauksen tarkastuskertomuksesta

Valtiontalouden tarkastusvirasto VTV on pyytänyt lausuntoa tarkastuskertomusluonnoksesta, joka liittyy valtionhallinnon kybersuojauksen järjestämiseen sekä luonnoksessa esitettyihin kannanottoihin. Turvallisuuskomitean sihteeristö esittää lausuntonaan seuraavaa:

Luonnos on hyvin jäsennelty ja siinä on tarkoituksenmukaisesti otettu kantaa keskeisiin kansalliseen kyberturvallisuuteen liittyviin asiakokonaisuuksiin ja niihin vaikuttaviin seikkoihin. Sihteeristö yhtyy luonnoksen näkemyksiin siinä, että kyberturvallisuuteen liittyvissä tilanteissa vastuusuhteet valtionhallinnossa ovat monimutkaiset, mikä aiheuttaa tarpeetonta viivettä häiriötilanteisiin reagoimisessa. Lisäksi häiriötilanteissa sekä ylipäätään kyberturvallisuuteen liittyvien tehtävien hoidossa on useasti tarve hallinnonalarajat ylittävään kokonaisvaltaiseen tilanteen hallintaan. Niin ikään virastokohtainen budjetointi hankaloittaa määrärahojen kohdentamista kokonaisuuden kannalta tärkeimpiin kehittämiskohteisiin. Yleisesti ottaen määrärahojen niukkuus rajoittaa kansallisen kyberturvallisuuden kehittämistä paitsi kokonaisuutena, myös hallinnonaloilla.

VTV:n lausuntopyynnön saatteessa on todettu, että lopullinen tarkastuskertomus tulee aikanaan olemaan julkinen asiakirja, vaikka nyt nähtävillä oleva luonnos ei sitä ole. Turvallisuuskomitean sihteeristö kiinnittää huomiota siihen, että useassa kohdin luonnosta kuvataan, mm. Valtorin toiminnan kuvauksen yhteydessä (s.23), valtionhallinnon kyberturvallisuuden puutteita sellaisella avoimuudella, jota ei voi suositella käsiteltäväksi julkisesti (JulkL 621/1999 24.1§:n 8 k).

VTV on luonnoksessaan käyttänyt termejä "kybersuojaus" ja "kyberloukkaus" sellaisissa yhteyksissä, joissa yleisesti käytetään sellaisia ilmaisuja kuin "kyberturvallisuus", "kyberhäiriötilanne" tai "kyberhyökkäys". Olisi toivottavaa, että tarkastuskertomuksessa käytetty termistö olisi yhdenmukainen käytössä olevien vallitsevien ilmausten kanssa. Tämän lisäksi kyberpuolustus-termi (s. 12) on varattu tarkoittamaan kyberturvallisuuden maanpuolustuksellista osa-aluetta, mikä ei sihteeristön mielestä sovi käytettäväksi puhuttaessa valtionhallinnon kyvystä suojata toimintojaan.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Edellisten termistöhuomioiden tueksi voimme hyvillä mielin todeta (s.15), että kyberturvallisuussanastoon liittyvä hanke on käynnistetty Turvallisuuskomitean johdolla, HVK:n rahoittamana ja Sanastokeskuksen tuottamana. Sanaston on tarkoitus valmistua keväällä 2018.

Pääsihteeri Vesa Valtonen

Erikoistutkija Pentti Olin

Jakelu Valtiontalouden tarkastusvirasto

Tiedoksi Turvallisuuskomitean puheenjohtaja Jukka Juusti

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, Internet
e-post, Internet
e-mail, Internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Valtiontalouden tarkastusvirasto

Viite: VTV:n lausuntopyyntö 21.6.2017 Dnro 185/54/2017

Lausunto tarkastuskertomusluonnoksesta Kybersuojauksen järjestäminen

Valtiovarainministeriö ilmoittaa pyydettynä lausuntonaan seuraavaa.

Tarkastuskertomusluonnoksessa nostetaan esille niitä seikkoja, joilla voidaan varmistaa ja kehittää valtionhallinnon kybersuojauksen vaikuttavuutta ja taloudellisuutta tarkoituksenmukaisella tavalla.

Valtiovarainministeriö huomioi esitetyt kannanotot sekä suositukset kehittäessään ohjausta vaikuttaen siten valtionhallinnon kybersuojauksen tuloksellisuuteen, vaikuttavuuteen ja taloudellisuuteen.

Yleisiä huomioita

Valtiovarainministeriöllä on merkittävä rooli julkisen hallinnon ICT-palveluiden tietoturvallisuuden, "kybersuojauksen" kehittämisen ohjaajana. Valtiovarainministeriö on tunnistanut useimmat tarkastuskertomusluonnoksessa esille sen toimintaan liittyvät havainnot ja kannanotot, joiden osalta kehittämistoimenpiteet ovat osittain etenemässä. Osa näistä kytkeytyy valtiovarainministeriön vastuulla oleviin Suomen kyberturvallisuusstrategian toimeenpano-ohjelman v. 2017-2020 toimenpiteisiin, osa julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) v. 2017-2019 toimintasuunnitelmaan ja osa valtiovarainministeriön vastuulla olevien valtionhallinnon yhteisten palveluiden tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjaamisen kehittämiseen.

Valtiovarainministeriö toivoo, että tarkastuskertomuksessa käytettävä terminologia olisi yhdenmukainen jo vakiintuneiden tieto- ja kyberturvallisuuteen liittyvän terminologian kanssa. Näitä on määritelty esimerkiksi Suomen Kyberturvallisuusstrategiassa sekä Suomen Pelastusalan Keskusjärjestö SPEKin Kokonaisturvallisuuden sanastossa. Tässä yhteydessä kybersuojaus (määritelmät sivulla 9) sekä kyberloukkaus ja kyberloukkaustilanne näyttäytyvät kapeasti laajemman tietoturvallisuuden osa-alueeksi.

Taustatietoa

Valtiovarainministeriön tehtävät

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Valtiovarainministeriön toimivalta tietoturvallisuuden ja tietohallinnon ohjauksessa ja kehittämisessä perustuu useisiin säädöksiin. Tällaisia ovat laki julkisen hallinnon tietohallinnon ohjaamisesta (634/2011) sekä laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011). Valtiovarainministeriö vastaa turvallisuusverkkotoiminnan yleishallinnollisesta, strategisesta, taloudellisesta ja tieto- ja viestintäteknisen varautumisen, valmiuden

ja turvallisuuden ohjauksesta ja valvonnasta (10/2015). Valtiovarainministeriön vastuulla on laissa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä tarkoitettujen yhteisten palvelujen palvelutuotannon yleishallinnollinen, strateginen sekä tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjaus (1226/2013). Valtiovarainministeriön vastuulla on laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016). Nämä tehtävät on valtiovarainministeriössä vastuutettu JulkICT-osastolle.

Valtiovarainministeriöstä annetussa asetuksessa (610/2003) ja valtiovarainministeriön työjärjestyksessä on määritelty tarkemmin ministeriön eri osastojen ohjausvastuut.

Yksityiskohtaisemman huomiot

Näkemyksiä tarkastusviraston kannanottoihin

Valtiontalouden tarkastusvirasto toivoo, että lausunnossa esitetään näkemyksiä tarkastusviraston alustavista kannanotoista. Tarkastuskertomusluonnoksessa on nostettu esille viisi kannanottoa:

1) Laajavaikutteisen kyberloukkaustilanteen operatiivista johtamista ei ole määritelty

Sivulla 39 todetaan, että "Tieto- ja kyberpoikkeamien hallinta valtionhallinnossa on määritelty ja vastuutettu". Kuvassa 3 sivulla 41 "Kuvio 3: Tieto- ja kyberpoikkematilanteiden hallinta" on kuitenkin kuvattu voimassa oleva näiden tilanteiden hallintamalli.

Valtiovarainministeriö tuotti kesällä 2016 päättyneessä SecICT-hankkeessa valtionhallinnon käyttöön useita GovCERT-palveluita, joista yhtenä luotiin VIRT-toimintamalli (Virtual Incident Response Team) laaja-alaisten tieto- ja kyberturvallisuushäiriöiden hallintaan. Toimintamallia on hyödynnetty useassa tällaisessa tilanteessa ja sen kehittämistä jatketaan ja samoin tullaan selvittämään sen laajentamista muualle julkiseen hallintoon.

VIRT-toiminta on liitetty osaksi VAHTI-toimintaa ja valtiovarainministeriö kehittää yhteistyössä muiden vastuutahojen kanssa hallintamallia myös operatiivisen johtamisen kehittämisestä paremmin vastaamaan muuttuvaa toimintaympäristöä, jossa myös palvelukeskusten rooli huomioidaan paremmin.

2) Kyberturvallisuusstrategian tavoitteita on jäänyt toteutumatta

Kyberturvallisuusstrategia pitää sisällään kolme visiota, mutta tässä yhteydessä viitataan ilmeisesti sen toimeenpano-ohjelman ensimmäiseen versioon, joka koostui 74 toimeenpiteestä. Uusi toimeenpano-ohjelma vuosille 2017-2020 julkaistiin keväällä 2017.

3) Kybersuojauksen rahoitusratkaisujen tarkoituksenmukaisuus on epäselvä

Kannanotto on erittäin aiheellinen ja keskeinen edellytys tieto- ja kyberturvallisuuden kehittämiseksi digitaaliseen toimintaympäristöön kohdistuvien uusien uhkien tunnistamiseksi ja niistä tunnistettavien riskien hallitsemiseksi.

4) ICT:n organisoinnin muutoksissa pitäisi huomioida myös Kybersuojaus

Tieto- ja kyberturvallisuus, kuten myös tietosuoja tulisi sisäänrakentaa kaikkeen organisaation toimintaan. Tämän johdosta se tulisi ottaa huomioon kaikissa merkittävissä muutostilanteissa, ei pelkästään ICT:n organisoinnissa.

5) Kyberturvallisuuden operatiivisen tilannekuvan muodostamista on syytä parantaa

Jotta Viestintävirastossa toimiva Kyberturvallisuuskeskus voi saada operatiivisen tilannekuvan muodostamisessa tarvittavaa tietoa, edellyttää se näihin liittyvien häiriötilanteiden ilmoittamista heille. Valtiovarainministeriö on valmistellut tähän liittyvää ohjeistusta siten, että se saadaan liikkeelle syksyllä 2017. Osittain tämä asia parantuu myös EU:n yleisen -tietosuoja-asetuksen toimeenpanon avulla (artikla 33, "Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle"), jossa tulee myös muutoksia näihin ilmoittamisvelvoitteisiin.

Kannanotot ovat hyvin valittuja, valtiovarainministeriö huomioi ne tähän kokonaisuuteen liittyvää toimintaa ohjatessaan ja kehittäessään.

Tarkastusviraston suositukset

Tarkastusluonnoksen neljästä suosituksesta kolme liittyy valtiovarainministeriön toimintaan ja yksi Valtoriin, jonka ohjausvastuu kuuluu valtiovarainministeriölle.

- *valtiovarainministeriö määrittelee laajavaikutteisen kyberloukkaustilanteenhallintaan operatiivisen johtamisen prosessin*

Ehdotus suosituksen otsikoksi:

- *valtiovarainministeriö määrittelee ja toteuttaa valtionhallinnon ICT-palveluiden osalta kyberhäiriötilanteiden operatiivisen hallinta- ja johtamismallin*

Tämän suosituksen osalta on jo aikaisemmin ryhdytty toimenpiteisiin. Suomen kyberturvallisuusstrategian toimeenpano-ohjelman v. 2017-2020 toimenpiteinä ovat:

> "Julkisen hallinnon kyberhäiriötilanteiden operatiivinen hallintamalli on toteutettu ja toiminnassa
>
> Liittyy strategiseen linjaukseen: 1,2,3,4,5,9
>
> Vastuutaho: Valtiovarainministeriö, liikenne- ja viestintäministeriö, Valtion tieto- ja viestintätekniikkakeskus Valtori
>
> Suomen kyberturvallisuusselvityksessä 2017 todetaan:
>
> Suomessa on viime vuosien aikana kehitetty kyberturvallisuuden tilannekuvan muodostamista sekä eri toimijoiden keräämien tietojenvaihtoa, mutta tietojenvaihdon sekä havaintokyvyn parantaminen on edelleen Suomessa kehitettävä asia kyberturvallisuudessa. On myös tärkeää, että esimerkiksi tietoisuutta havaituista haavoittuvuuksista jaetaan aktiivisesti eri toimijoiden välillä, ja mahdollisista tietomurroista ilmoitetaan luottamuksellisella tavalla, jotta vastaavien tietomurtojen estäminen muualla yhteiskunnassa mahdollistuu.

Valtiovarainministeriön johdolla Valtori yhdessä liikenne- ja viestintäministeriön, Viestintäviraston ja muiden toimijoiden kanssa suunnittelee edelleen kehitetyn poikkihallinnollisen kyberhäiriötilanteiden operatiivisen hallintamallin ja havainnointikyvyn (VIRT), joka sisältää kuvauksen tietovirroista ja toimintaprosesseista julkisen hallinnon ja elinkeinoelämän välillä merkittävissä julkisen hallinnon kyberhäiriö-, ja tietoturvapoikkeamatilanteissa. Toteutetaan tutkimushankkeena kybertilannekuvan ja analysointikyvykkyyden kehittäminen.

Niiltä osin, kuin toimijat eivät kuulu NIS- direktiivin ilmoitusvelvollisten piiriin, valtiovarainministeriö varmistaa, että ministeriöt, hallinnonalat ja palvelukeskukset sekä maakunta- ja kuntatoimijat ja niiden omistamat yritykset ilmoittavat Viestintävirastolle julkisen hallinnon toimintaa ja palveluita koskevista kyberhäiriötilanteista sekä tietoturvapoikkeamista. Ilmoitusvelvollisuus on otettava huomioon alihankkijoiden kanssa tehtävissä sopimuksissa. Valtiovarainministeriö ohjeistaa ilmoitusvelvollisuuden toteuttamisesta tarkemmin. Lisäksi toteutetaan sopimuksiin perustuva varautuminen yksityissektorin toimijoiden kanssa."

- *valtiovarainministeriö selvittää, miten ICT-palvelujen rakentamisen jälkeinen kybersuojaus tulisi ottaa huomioon valtion talousarvion määrärahoissa*

Ehdotus suosituksen otsikoksi:

- *valtiovarainministeriö selvittää, miten palvelujen kybersuojaus tulisi ottaa huomioon palveluiden koko elinkaaren rahoituksessa*

Valtiovarainministeriö huomioi suosituksen uudessa investointien ohjaus- ja rahoitusmallin toimeenpanossa.

- *Valtori parantaa kybersuojauksen menettelyjen ja kyberloukkausten havainnoinnin toteutusta, arviointia ja kehittämistä*

Tämä on yksi osin valtiovarainministeriön ja myös Valtorin vastuulla olevista kyberturvallisuusstrategian toimeenpano-ohjelman 2017-2020 kohteista, joita ollaan kehittämässä Valtorin sekä muiden valtiovarainministeriön hallinnonalan keskeisten valtion yhteisiä palveluita tuottavien virastojen kanssa. Toimenpiteen osalta todetaan:

"12) Yhteiskunnan elintärkeille toiminnoille välttämättömät julkisen hallinnon digitaaliset palvelut sekä niiden tarvitsema infrastruktuuri on tunnistettu ja hallinnassa

Liittyy strategiseen linjaukseen: 3,4,5,6,9
Vastuutaho: Valtiovarainministeriö, Valtion tieto ja viestintätekniikkakeskus, muut julkishallinnolle palveluita tuottavat palvelukeskukset ja yritykset"

- *valtiovarainministeriö parantaa kybersuojausta palvelevan operatiivisen tilannekuvan muodostamista ohjeistamalla viranomaisia ilmoittamaan kyberloukkauksista Kyberturvallisuuskeskukselle*

Tätä on sivuttu jo tässä lausunnossa aikaisemmin tarkastusviraston kannanottojen yhteydessä.

Sivu 27

"TUVE-ympäristö on varautumiseltaan korotetun tason ratkaisu, mutta tarkoitettu vain turvallisuusviranomaisten käyttöön."

Tulkinta siitä, että TUVE-ympäristö olisi tarkoitettu vain turvallisuusviranomaisten käyttöön on virheellinen. Esitetään tekstin muuttamista TUVE-lain (10/2015) 1§:ää vastaavaksi "tarkoitettu valtion ylimmän johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten ja muiden den käyttöön". Huomioitavaa tässä on myös se, että Valtorilla on palveluntuottajana oikeus käyttää TUVEa. Käyttövelvoitetta ja muuta käyttöä tarkennetaan TUVE-lain 3 ja 4 pykälissä.

Myös TUVE-ympäristön varautumistason osalta tulisi käyttää TUVE-lain määritelmää. Tulkinta siitä, että TUVE:n varautumistaso on korotettu, vaatii perustelut, sillä lain mukaisesti "Turvallisuusverkko on valtion omistuksessa ja hallinnassa oleva tietoyhteiskuntakaaressa (917/2014) tarkoitettu viranomaisverkko, joka täyttää korkean varautumisen ja turvallisuuden vaatimukset siten kuin siitä laissa erikseen säädetään tai lain nojalla määrätään.

Edellä olevan lisäksi valtiovarainministeriö esittää erillisessä liitteessä teknisluonteisia täsmennysehdotuksia tarkastuskertomusluonnokseen.

Ylijohtaja, ICT-johtaja — Anna-Maija Karjalainen

Tietohallintoneuvos, yksikön päällikkö — Aku Hilve

Liite 1
Liite valtiovarainministeriön lausuntoon VM/1398/00.05.00/2017 , VTV:n lausuntopyyntö 21.6.2017 Dnro 185/54/2017, Teknisluonteiset huomiot ja korjaukset

21.8.2017

Dnro:
1017/04/2017

Valtiontalouden tarkastusvirasto

Viestintäviraston lausunto tarkastuskertomusluonnoksesta kybersuojauksen järjestämisestä (Dnro 185/54/2016)

Valtiontalouden tarkastusvirasto on pyytänyt Viestintävirastoa antamaan lausunnon tarkastuskertomusluonnoksesta kybersuojauksen järjestämisestä. Lausuntopyynnön tarkoituksena on erityisesti varmistaa, että kertomukseen ei sisälly asia- tai tulkintavirheitä, joilla olisi vaikutusta tarkastuksen kannanottoihin, sekä kuulla Viestintäviraston näkemys tarkastusviraston alustavista kannanotoista. Teknisluonteiset korjaus- ja täsmennysehdotukset on pyydetty antamaan erikseen.

Viestintävirasto kiittää mahdollisuudesta lausua asiasta ja lausuu seuraavaa:

Viestintävirasto pitää luonnosta tarkastuskertomusta hyvin jäsenneltynä ja yhteiskunnallisesti vaikuttaviin asioihin painottuvana. Tehdyt kannanotot ja suositukset ovat perusteltuja.

Yleistä

Yhteiskunnan kokonaisvaltaisen suojautumisen näkökulmasta keskeisiä puutteita arvioidaan olevan havainnointikyvyssä, tilannekuvassa ja tilanneymmärryksessä sekä laaja-alaisten hyökkäysten torjunnassa. Tällä hetkellä kyetään hallitsemaan pieniä ja keskisuuria tietoturvauhkia, mutta vakavien ja laaja-alaisten hyökkäysten torjuntakyky on heikompi.

Tarkastuskertomuksessa on kiinnitetty huomiota kyberturvallisuusstrategian toimeenpano-ohjelman täytäntöönpanoon liittyviin haasteisiin. Asiaa on tarkasteltu myös Suomen kyberturvallisuuden nykytilaa, tavoitetilaa ja tarvittavia toimenpiteitä tavoitetilan saavuttamiseksi kartoittavassa selvityksessä. Selvityksen mukaan yksi strategian onnistumisista on ollut Kyberturvallisuuskeskuksen perustaminen.

Viestintävirasto yhtyy vahvasti kertomuksessa esitettyyn näkemykseen siitä, että sen toiminnan tuloksellisuus perustuu myös jatkossa vahvaan uudistuvaan osaamiseen, Kyberturvallisuuskeskusta kohtaan tunnettuun luottamukseen, verkostoitumiseen ja toiminnalliseen ketteryyteen. Näistä tulee kriittisiä vaatimuksia Kyberturvallisuuskeskuksen toimintapuitteille – kuten brändille, toimivallalle ja vetovoimalle alan huippuammattilaisten työpaikkana.

Viestintävirasto
Kommunikationsverket
Finnish Communications Regulatory Authority

Itämerenkatu 3 A
PL 313
00181 Helsinki
Puhelin 0295 390 100
www.viestintävirasto.fi

Östersjögatan 3A
PB 313, FI-00181
Helsingfors, Finland
Telefon +358 295 390 100
www.kommunikationsverket.fi

Itämerenkatu 3A
P.O. Box 313, FI-00181
Helsinki, Finland
Telephone +358 295 390 100
www.ficora.fi

Kyberturvallisuuden operatiivisen tilannekuvan muodostamista on syytä parantaa

Viestintäviraston kyberturvallisuuskeskus pitää yllä kyberturvallisuuden kansallista tilannekuvaa. Mitä kattavampi tilannekuva on, sitä paremmin se palvelee kybersuojauksen järjestämistä. Kyberhyökkäyksen kohteeksi joutuneilla valtionhallinnon toimijoilla ei ole tällä hetkellä ilmoitusvelvollisuutta Viestintävirastolle.

Tarkastuskertomuksessa ehdotetun mukaisesti Valtiohallinnon organisaatioiden velvoittaminen ilmoitusten tekemiseen parantaisi tilannekuvan laatua ja koko yhteiskunnan saamaa lisäarvoa.

Kybersuojauksen rahoitusratkaisujen tarkoituksenmukaisuus on epäselvä

Digitaalinen yhteiskunta ei tule rakentumaan luotettavaksi ja toimintakykyiseksi ilman riittävän tietoturvallisuuden, toimintavarmuuden tai yksityisyyden suojan varmentamista. Digitaalisuuden tuomat uudenlaiset palvelukonseptit, toiminta-alustat, ekosysteemit ja erilaisten palvelumuotoilujen saumaton yhteentoimivuus vaativat uudenlaista turvallisuuden varmistamista ja toimintakehikkoa.

Viestintäviraston valtionhallinnolle tarjoamat GovCERT-palvelut rahoitetaan valtiovarainministeriön Viestintävirastolle osoittamalla sopimusperusteisella rahoituksella. Viestintäviraston arvion mukaan sillä ei ole nykyisten rahoitusjärjestelyiden perusteella käytettävissään riittäviä resursseja tilanteessa, jossa valtionhallintoon kohdistuu yhtäaikaisesti useampia vakavia ja laaja-alaisia tietoturvaloukkauksia.

Viestintävirasto on vuoden 2017 alussa ehdottanut vuotuista 5 miljoonan euron lisäystä rahoitukseensa mahdollistamaan digitalisaatiokehityksen tehokas tukeminen. Viestintävirastolle osoitettiin 2 miljoonan euron vuosittainen lisämääräraha tietoturvallisuuden, toimintavarmuuden ja yksityisyydensuojan varmentamiseksi ja kehittämiseksi.

VRK/Pekka Rehn, Ristimäki Pekka

21.8.2017

LAUSUNTO

Viitteet:

Lausuntopyyntö Dnro 185/54/2016 Tarkastuskertomusluonnos Kybersuojauksen järjestäminen
Lausuntopyyntö Dnro 340/54/2015 Tarkastuskertomusluonnos Sähköisten palveluiden toimintavarmuuden ohjaus

VRK/Pekka Rehn, Ristimäki Pekka

21.8.2017

Sisällysluettelo

VRK/Pekka Rehn, Ristimäki Pekka

21.8.2017

LAUSUNTO

1 Johdanto

Väestörekisterikeskus (VRK) kiittää Valtiontalouden tarkastusvirastoa ja sen johtavia tuloksellisuustarkastajia Pirkko Lahdelmaa ja Pasi Korhosta hyvistä havainnoista ja kannanotoista sekä tarkastuksen aikana että tarkastuskertomuksessa. Tarkastus antoi hyvän kuvan kohdealueesta. Erityisen arvokasta oli nostaa osin uusi vaatimus toimia hyvinkin nopeasti verkottuneessa ja nopeasti muuttuvassa toimintaympäristössä ja tuoda selkeästi esiin ettei normaalitilanteessa hyvät toimintatavat pysty välttämättä vastaamaan voimakkaasti integroituneen ympäristön poikkeustilanteiden asettamiin vaatimuksiin.

2 Kybersuojauksen järjestäminen

Sivu 24 (sivun reuna) :

”VRK katsoo Valtorille keskitettyjen tietoturvakontrollien rahoitusongelmien olevan syy VRK:n pirstaloituneeseen kyberturvallisuuden tilannekuvaan”

Täsmennys:

”VRK katsoo Valtorille keskitettyjen tietoturvakontrollien ja Valtorin SSOC:n rahoitusongelmien olevan yksi syy VRK:n pirstaloituneeseen kyberturvallisuuden tilannekuvaan”

Sivu 24:

”VRK:n mukaan Valtori ei ole onnistunut tuottamaan Valtorin palveluiden yhteistä tilannekuvaa asiakasvirastoille ja Kyberturvallisuuskeskukselle. Valtorin tietoturvavalvomon ja Kyberturvallisuuskeskuksen näkyvyys VRK:n palveluihin on huono. VRK:lla pitäisi olla käytössään tietoturvavalvomopalvelu, eikä Valtorin SSOC kata laajasti VRK:n palveluja. VRK:n mukaan valtion tietoturvavalvomotoiminta olisi kuitenkin kustannustehokasta keskittää Valtorin SSOC-toimintoon. VRK katsoo, että jos asiakasmaksuilla tapahtuva rahoitus ei mahdollista laajempaa toimintaa, ratkaisuna voisi olla keskitetty rahoitus.”

Täsmennys:

”VRK:n mukaan Valtori ei ole onnistunut tuottamaan asiakasvirastoille riittävää tilannekuvaa Valtorin palveluiden (TORI) keskeisten kyberturvallisuuteen liittyvien tapahtumien osalta. Valtorin tietoturvavalvomon ja Kyberturvallisuuskeskuksen näkyvyys VRK:n palveluihin (TOSI) ei ole riittävä. VRK:lla pitäisi olla käytössään tietoturvavalvomopalvelu, eikä Valtorin SSOC kata laajasti VRK:n palveluja. VRK:n mukaan valtion tietoturvavalvomotoiminta olisi kuitenkin kustannustehokasta keskittää Valtorin SSOC-toimintoon. VRK katsoo, että jos asiakasmaksuilla tapahtuva rahoitus ei mahdollista laajempaa toimintaa, ratkaisuna voisi olla keskitetty rahoitus.

Valvonta on tehokas toteuttaa keskitetysti mutta keskitetyllä toimijalla ei ymmärrettävästi ole osaamista TOSI-palveluiden valvottavista kohteista ja tapahtumista. Tämä edellyttää yhteistyötä jossa asiakasvirasto yhdessä toteuttajan kanssa määrittelee, luo ja jatkuvasti ylläpitää valvontaa”

VRK/Pekka Rehn, Ristimäki Pekka

21.8.2017

Sivu 36:
"Sertifiointi ei vielä kata KaPA- palveluita..."

Kommentti: KaPa-palveluiden asemesta voi käyttää termiä "Suomi.fi-palvelut" (KaPa-palvelut ovat nykyään Suomi.fi-palveluita).

Sivu 37:

"VRK:lla on käytännön ohjeistusta sovelluskehityksen tietoturvasta, ja tietoturva-asiantuntijat ovat koko ajan mukana kehittämisessä ja konsultoitavissa. Kehityksen lomassa ja vielä ennen käyttöönottoa arvioidaan tietoturvaa ja tietoturva-auditoidaan palveluita. VRK käyttää arviointeihin ulkoisia asiantuntijoita."

Täsmennys:

"VRK:lla on käytännön ohjeistusta sovelluskehityksen tietoturvasta, ja tietoturva-asiantuntijat ovat mukana kehittämisessä ja konsultoitavissa. Tietoturvatestausta tehdään osana ketterää sovelluskehitystä. Ennen sovelluksen/palvelun käyttöönottoa suoritetaan tarpeellisin osin tietoturva-auditointi. VRK käyttää tietoturvatestaukseen ja -auditointeihin ulkoisia asiantuntijoita."

Sivu 40:

"VRK tiedottaa tietoturvaloukkaustilanteessa asiakkaille, osallistuu virka-aikaan häiriön selvitykseen ja tarjoaa sovellustason osaamista käyttöpalvelutoimittajalle. VRK osallistuu VIRT-kokouksiin."

Täsmennys:

"VRK koordinoi tietoturvapoikkeamien selvitystä ja vastaa niistä tiedottamisesta viranomaisille (esim Kyberturvallisuuskeskus) ja asiakkaille sekä muille sidosryhmille poikkeamanhallinta- ja kriisiviestintäohjeistusten mukaisesti. Vakavista tietoturvapoikkeamista ilmoitetaan aina Kyberturvallisuuskeskukselle. VRK osallistuu VIRT-kokouksiin."

3 Sähköisten palveluiden toimintavarmuuden ohjaus

Sivu 5:

"Toiminta-arkkitehtuuri ja strateginen palveluajattelu kehittäisivät toimintavarmuuden suunnittelua ja laajentaisivat näkökulmaa tietohallinnon ulkopuolelle."

Kommentti:

Toiminta-arkkitehtuuri laajentaa näkökulmaa vain, jos tosiallisen toiminta-arkkitehtuuri-työn tekevät tietohallinnon ulkopuoliset henkilöt.

Sivu 36:

"Väestörekisterikeskus otti käyttöönsä vuoden 2016 alussa tietoturvallisuuden tilannekuva- ja toiminnanohjausjärjestelmän Graniten, jolloin myös riskienhallintaprosessi ja -järjestelmä uudistettiin. Graniteen muodostetaan muun muassa riskirekisterit ja hallintajärjestelmät. Tarkastuksen aikana riskienhallintaa ohjasivat Väestörekisterikeskuksen riskienhallintapolitiikka ja riskienhallinnan vuosikello. Riskienhallinnan vuosikello oli välittynyt tietoturvallisuuden hallintajärjestelmän ja yksiköiden tietoturvallisuuden vuosikelloon. Tietoriskejä hallitaan osana viraston kokonaisvaltaista riskienhallintaa. Palvelujen riskienarviointi tehtiin muutamaa lievää poikkeusta lukuun ottamatta riskienhallinnan vuosikellon mukaisesti, mutta

riskienhallinnan toimenpiteitä ei kaikin osin pystytty toteuttamaan aikatauluissaan. Vuoden 2016 aikana oli pyritty vakiinnuttamaan riskienhallinnan käytäntöjä, mutta esimerkiksi tietoturvaryhmän syyskuun kokouksessa havaittiin, että kaikki eivät olleet pitäneet Graniten tietoja riskienhallinnan tehtävistä ajan tasalla. Johdon katselmoinnissa käytiin läpi riskienarvioinnin tuloksia. Tuolloin keskustelua herätti kirjausten taso ja riskien liiallinen määrä. Tunnistettiin tarve keskittyä jatkossa hallintatoimien ja resurssien suuntaamisen näkökulmasta merkittävimpiin riskeihin. Väestörekisteri-keskus itse raportoi riskienhallinnan integroituvan entistä vahvemmin osaksi normaalia liiketoiminnan johtamista."

Kommentti: Granite on tuotenimi, joten ehdotuksena uusi muotoilu.

Uusi muotoilu:

"Väestörekisterikeskus otti käyttöönsä vuoden 2016 alussa tietoturvallisuuden tilannekuva- ja toiminnanohjausjärjestelmän , jolloin myös riskienhallintaprosessi ja -järjestelmä uudistettiin. Järjestelmään muodostetaan muun muassa riskirekisterit, hallitaan vaatimustenmukaisuutta sekä tietoturva- ja auditointipoikkeamia. Tarkastuksen aikana riskienhallintaa ohjasivat Väestörekisterikeskuksen riskienhallintapolitiikka ja riskienhallinnan vuosikello. Riskienhallinnan vuosikello oli välittynyt tietoturvallisuuden hallintajärjestelmän ja yksiköiden tietoturvallisuuden vuosikelloon.Tietoriskejä hallitaan osana viraston kokonaisvaltaista riskienhallintaa. Palvelujen riskienarviointi tehtiin muutamaa lievää poikkeusta lukuun ottamatta riskienhallinnan vuosikellon mukaisesti, mutta riskienhallinnan toimenpiteitä ei kaikin osin pystytty toteuttamaan aikatauluissaan. Vuoden 2016 aikana oli pyritty vakiinnuttamaan riskienhallinnan käytäntöjä, mutta esimerkiksi tietoturvaryhmän syyskuun kokouksessa havaittiin, että kaikki eivät olleet pitäneet tietoja riskien hallintatoimista ajan tasalla.168 Johdon katselmoinnissa käytiin läpi riskienarvioinnin tuloksia. Tuolloin keskustelua herätti kirjausten taso ja aktiivisten riskien liiallinen määrä (hallintatoimet kesken tai jäännösriskiä ei oltu hyväksytty). Tunnistettiin tarve keskittyä jatkossa hallintatoimien ja resurssien suuntaamisen näkökulmasta merkittävimpiin riskeihin. Väestörekisteri-keskus itse raportoi riskienhallinnan integroituvan entistä vahvemmin osaksi normaalia liiketoiminnan johtamista."

Sivu 36:

"Tuolloin keskustelua herätti kirjausten taso ja riskien liiallinen määrä. Tunnistettiin tarve keskittyä jatkossa hallintatoimien ja resurssien suuntaamisen näkökulmasta merkittävimpiin riskeihin. Väestörekisteri-keskus itse raportoi riskienhallinnan integroituvan entistä vahvemmin osaksi normaalia liiketoiminnan johtamista."

Täsmennys:

"Tuolloin keskustelua herätti kirjausten taso ja aktiivisten riskien liiallinen määrä (jäännösriski jäänyt hyväksymättä, tai hallintatoimet kesken). Tunnistettiin tarve keskittyä jatkossa hallintatoimien ja resurssien suuntaamisen näkökulmasta merkittävimpiin riskeihin sekä kiinnittää huomiota riskien yhteismitallisuuteen. Väestörekisterikeskus itse raportoi riskienhallinnan integroituvan entistä vahvemmin osaksi normaalia liiketoiminnan johtamista."

Helsingissä 21.8.2017

Lea Krohns
Ylijohtaja

Pekka Rehn
Johtaja
Esittelijä

Trafi Liikenteen turvallisuusvirasto
Trafiksäkerhetsverket

LAUSUNTO

VTV
tuloksellisuustarkastus@vtv.fi

Päiväys/ Datum 30.08.2017

Dnro/Dnr TRAFI/

Viite/ Referens Lausuntopyyntö 22.6.2017
Dnro 185/54/2016

Lausunto Tarkastuskertomusluonnoksesta Kybersuojauksen järjestäminen

Valtiontalouden tarkastusvirasto lähettää oheisena luonnoksen tarkastuskertomukseksi ja pyytää antamaan siitä lausunnon. Lausuntopyynnön tarkoituksena on erityisesti varmistaa, että kertomukseen ei sisälly asia- tai tulkintavirheitä, joilla olisi vaikutusta tarkastuksen kannanottoihin, sekä kuulla näkemykset tarkastusviraston alustavista kannanotoista.

Liikenteen turvallisuusvirasto (Trafi) on tarkastellut luonnosta ja esittää seuraavat huomiot.

Tarkastusviraston kannanotot

Tarkastusvirasto suosittaa tarkastuskertomuksessaan seuraavia asioita:

1. valtiovarainministeriö määrittelee laajavaikutteisen kyberloukkaustilanteen hallintaan operatiivisen johtamisen prosessin
2. valtiovarainministeriö selvittää, miten ICT-palvelujen rakentamisen jälkeinen kybersuojaus tulisi ottaa huomioon valtion talousarvion määrärahoissa
3. Valtori parantaa kybersuojauksen menettelyjen ja kyberloukkausten havainnoinnin toteutusta, arviointia ja kehittämistä
4. valtiovarainministeriö parantaa kybersuojausta palvelevan operatiivisen tilannekuvan muodostamista ohjeistamalla viranomaisia ilmoittamaan kyberloukkauksista Kyberturvallisuuskeskukselle

Trafi tukee Tarkastusviraston suosituksia ja lisäksi painottaa seuraavaa: Kun Valtori parantaa kohdassa 3. mainittuja asioita, se tulee tehdä yhteistyössä Valtorin asiakasvirastojen kanssa. Näin varmistetaan virastojen kyberturvallisuustarpeiden huomioiminen Valtorin palvelukehityksessä.

Tarkastusvirasto kertoo kannanotoissaan että julkishallinnon ICT:n organisaatiomuutokset ovat vaikuttaneet kybersuojauksen järjestelyihin. Tämä vaikutus on ollut havaittavissa myös Trafissa sekä Valtorin että VRK:n palveluiden suhteen. Trafi toivoo että Valtori huolehtisi jatkossa tuottamiensa palveluiden kyberturvallisuudesta sekä tuottaisi toimialariippumattomia kyberturvallisuuspalveluja, joita virastot voisivat hyödyntää toiminnassaan koska niiden tuottaminen yksittäisen viraston toimesta ei ole kustannustehokasta (mm. SOC). Julkishallinnon yhteisistä palveluista myös Suomi.fi –palvelut ovat Trafin palvelutuotannon kannalta kriittisessä roolissa ja siten myös niiden kybersuojauksen järjestäminen on Trafin palveluiden jatkuvuuden näkökulmasta tärkeää.

Tarkastusvirasto kertoo kannanotoissaan myös että kyberloukkausten kohteilla ei ole nyt ilmoitusvelvollisuutta Kyberturvallisuuskeskukselle. Trafin kyberturvallisuustoimintamallien mukaisesti Trafi ilmoittaa jo nykyisellään kyberloukkauksista Kyberturvallisuuskeskukselle. Trafi kannattaa valtiohallinnon organisaatioiden velvoittamista ilmoitusten tekemiseen tilannekuvan laadun parantamiseksi.

Luku 2

Tarkastuskertomuksen luvussa 2.1 tarkastusvirasto kertoo valtionhallinnossa vastuusuhteiden olevan monimutkaisia ajatellen mahdollisten kyberloukkausten luonnetta, laajuutta ja toteutustapaa. Trafi näkee vastuusuhteiden selkeyttämisen tärkeänä asiana erityisesti huomioiden kyberturvallisuusympäristön jatkuvan monimutkaistumisen.

Tarkastuskertomuksen luvussa 2.2 tarkastusvirasto nostaa esille että VRK:lla pitäisi olla käytössään tietoturvavalvomopalvelu, eikä Valtorin SSOC kata laajasti VRK:n palveluja. VRK:n mukaan valtion tietoturvavalvomotoiminta olisi kuitenkin kustannustehokasta keskittää Valtorin SSOC-toimintoon. Koska Trafin sähköiset asiointipalvelut ovat riippuvaisia VRK:n ratkaisuista, niiden kyberturvallisuuden järjestäminen on Trafille kriittistä.

Luvussa 2.2. myös mainitaan, että siitä riippumatta, missä määrin kybersuojaus on hajautettua tai keskitettyä, jokaisen valtion viraston ja laitoksen ja niiden yhteistyötahojen tulee osaltaan pitää yllä ja kehittää kybersuojauksen edellytyksiään. Tämän vuoksi Trafissa on käynnistetty Digitaalinen turvallisuus –kehittämishanke, jonka alla Trafin digitaalisten palvelujen ja trafilaisten kyberturvallisuutta jatkokehitetään.

Luvussa 2.3 todetaan että monessakaan valtion virastossa ja laitoksessa ei ole omaa turvallisuustoimintokeskusta, tietoturvapäällikköä tai vastaavia avainhenkilötä. Trafissa on varautumispäällikkö ja kaksi täyspäiväistä kyberturvallisuusasiohin keskittyvää henkilöä Teknologiapalvelut-yksikössä. Lisäksi Trafin riskienhallintaa koordinoidaan Johtamisen tuki –yksikön toimesta.

Luku 4

Luvussa 4 kerrotaan että julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) toimii julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä. Yksi VAHTIn keskeinen tehtävä on laatia ja julkaista hallinnolle tietoturvaohjeita, joissa ohjeistetaan myös kybersuojauksen järjestämistä. VAHTI-ohjeita on kritisoitu siitä, että ne eivät kaikin osin vastaa valtionhallinnon ICT:n organisoinnin nykytilannetta eikä ohjeiden tarkkuustaso palvele kunnolla toiminnan järjestämistä. Liikenteen turvallisuusvirasto on samaamieltä VAHTI-ohjeista esitetystä kritiikistä.

Kappaleessa 4.2 kerrotaan että Trafilla sertifioitu ISO27001-järjestelmä ja se auditoidaan kolmen vuoden syklissä, ja vuonna 2016 tehtiin täysauditointi. Kertomuksessa mainitun sijaan täysauditointi tehtiin 2017.

Kappaleessa 4.2 kerrotaan että Trafilla on sertifioitu ISO27001-järjestelmä ja se o huomioitu toimittajasopimuksen tietoturvaliitteessä. Lisäksi Trafi haluaa korostaa, että kaikille Trafissa työskenteleville sovelluskehittäjille teetetään turvallisuusselvitys.

Lisäksi kappaleessa 4.2 kerrotaan että sovelluksiin tehdään tietoturvatestaus ennen käyttöönottoa ja jatkossa aina kun tulee sellaisia muutoksia, jotka voivat vaikuttaa tilanteeseen. Lisäksi Liikenteen turvallisuusvirasto on osallistunut hackathon-tapahtumaan syksyllä 2016, missä viraston sähköisten asiointipalveluiden turvallisuutta testattiin.

Juhani Nikula
Hallintojohtaja

Heidi Rantanen
Osastopäällikkö