Digiturvan hyvät käytännöt johdolle ja ICT:n sekä digiturvan asiantuntijoille – tarkistuslista

Versio 1.0

26.10.2020

VAHTI

26.10.2020

Digiturvan hyvät käytännöt johdolle ja ICT:n sekä digiturvan asiantuntijoille – tarkistuslista

Tämän tarkistuslistan tarkoitus on nostaa esille, kuinka julkisen hallinnon ja muiden suomalaisten organisaatioiden tulisi ottaa huomioon uudenlainen uhkatilanne, joka johtuu tietoverkkorikollisten toiminnassa tapahtuneesta muutoksesta.

Viimeisten vuosien aikana entistä suuremmaksi organisaatioiden toimintaa ja jatkuvuutta uhkaavaksi tekijäksi ovat nousseet ns. lunnashaittaohjelmahyökkäykset (ransomware attacks). Tämä globaali ilmiö on koettu viime vuosina myös Suomessa. Erityisesti kesällä 2019 Kokemäen kaupunkiin kohdistuneesta onnistuneesta hyökkäyksestä on jaettu paljon hyviä oppeja.

Tietoverkkorikolliset ovat havainneet, että organisaatiot eivät maksa vaadittuja lunnaita. Organisaatioilla on kyvykkyys palautua hyökkäyksestä palauttamalla tietojärjestelmät ja tiedot esimerkiksi varmuuskopioilta. Siksi tässä hyökkäysmallissa on tapahtunut vuoden 2020 aikana selkä muutos.

Olemme jo alkuvuodesta 2020 varoittaneet eri tilaisuuksissa, että tietoverkkorikolliset eivät tyydy vain palveluiden lamauttamiseen ja tietojen salaamiseen, vaan sen lisäksi he varastavat palveluissa olevat tiedot. Mikäli organisaatio ei edelleenkään suostu maksamaan lunnasvaatimuksia, tietoverkkorikolliset tehostavat uhkausta kertomalla, että he aikovat julkaista salassa pidettäviä tietoja, henkilötietoja tai erityisiin tietoryhmiin kuuluvia ns. arkaluonteisia henkilötietoja julkisuuteen.

Tämä sama havainto on nostettu esille Liikenne- ja viestintävirastossa toimivan Kyberturvallisuuskeskuksen Kybersää-katsauksissa. Globaalisti tällaisista hyökkäyksistä on ollut jo useita esimerkkejä, ja nyt tällaiset hyökkäykset ovat rantautuneet myös Suomeen.

Tämä hyvät käytännöt -asiakirja on suunnattu organisaatioiden johdolle ja ICT-palveluiden ja digiturvan parissa työskenteleville asiantuntijoille. Tarkistuslistalla on asioita, joiden tulisi olla osa organisaation toiminnan arkea. Listalle on koottu periaatteita ja hyviä käytäntöjä, joita on nostettu esille jo useamman vuoden ajan. Lisäksi asiakirjan loppuun on koottu linkkejä tähän aihepiiriin liittyviin viranomaisohjeisiin.

Tämä asiakirja julkaistaan osana Digiturvaviikon 26.-30.10.2020 tukimateriaaleja. Asiakirjan on tuottanut ja sen sisällöstä vastaa Digi- ja väestötietovirastossa toimiva Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) yhteistyössä digitaalisen turvallisuuden keskeisten virastojen ja asiantuntijoiden kanssa.

Lisätietoja:
Kimmo Rousku, VAHTI-pääsihteeri, kimmo.rousku@dvv.fi, puh. 0295 535 120

Tarkistuslista organisaatioiden johdolle

Julkisen hallinnon organisaation johdon tehtävä ja vastuu on huolehtia organisaation tuottamien palveluiden turvallisuudesta ja sen käsittelemien tietojen turvaamisesta. Johto voi käyttää apuna organisaation toiminnan tarkistamisessa ja kehittämisessä seuraavaa yhdeksänkohtaista tarkistuslistaa:

1. Organisaatiossa tiedetään, mitkä ovat organisaatiota koskevat lakisääteiset velvoitteet, mukaan lukien erityislainsäädännöstä tulevat tehtävät organisaation tuottamia tai sen käsittelemiä tietoja koskien. Tässä tulee huomata erityisesti kaksi seuraavaa kohtaa:

   - Organisaatio täyttää 25.5.2018 sovellettavaksi tulleen EU:n yleisen tietosuoja-asetuksen ja 1.1.2019 voimaan astuneen Tietosuojalain velvoitteet.

   - Organisaatio toteuttaa 1.1.2020 voimaan astunutta Tiedonhallintalakia, jossa sekä julkisella hallinnolla että muilla lain piiriin kuuluvilla organisaatioilla on eri tasoisia siirtymäkausia lain soveltamisen osalta. Toimivaltaisena viranomaisena tässä toimii tiedonhallintalautakunta, jonka verkkosivuilta löytyvät lautakunnan suositukset ja ohjeet.

2. Organisaatio on arvioinut toimintaansa ja palveluihinsa liittyvät uhkat ja tunnistanut toimintaan liittyvät kriittiset riskit sekä ottanut riskit hallintaan toteuttamalla suunnitellut hallintatoimenpiteet. Näiden riskien tilaa ja uusien uhkien kehittymistä seurataan säännöllisesti.

   Ohje riskienhallintaan

3. Organisaatio on varautunut sen toimintaan liittyviin häiriöihin laatimalla suunnitelmat toiminnan jatkuvuudesta, varautumisesta ja valmiudesta.

   Toiminnan jatkuvuuden hallinta

   Tietoturvapoikkeamatilanteiden hallinta

   Yhteiskunnan turvallisuusstrategia 2017

   Organisaatio harjoittelee säännöllisesti häiriötilanteiden hallintaa.

   - Suosittelemme osallistumista TAISTO20-harjoitukseen 12.11. tai 19.11.2020. Vuoden 2018 harjoituksessa käsiteltiin henkilötietojen päätymistä julkisuuteen tietomurron seurauksena. Vuoden 2019 harjoituksessa käsiteltiin verkkohyökkäystä, jonka osana tietoverkkorikolliset esittivät lunnasvaatimuksen. Koska lunnasvaatimuksiin ei tule suostua, rikolliset lamauttivat organisaation kriittiset tietojärjestelmät.

4. Organisaatio luokittelee tuottamansa tai ulkopuolelta saamansa tiedot – esimerkiksi julkinen / salassa pidettävä / turvallisuusluokiteltu tieto (valtionhallinto) – sekä edellä mainittuihin sisältyvät henkilötiedot. Henkilötiedoista tunnistetaan ja tiedetään, mitkä ovat erityisiin tietoryhmiin kuuluvia, ns. arkaluonteisia henkilötietoja.

   Lisäksi organisaatio on määrittänyt, ohjeistanut ja kouluttanut henkilöstölle ja ulkoisille palveluntuottajille, missä palveluissa ja millä työvälineillä edellä tunnistettuja tietoja on sallittua käsitellä.

5. Palveluita hankkiva tai ulkoistava organisaatio sisällyttää turvallisuuteen liittyvät hankintavaatimukset osaksi laadittavaa palvelusopimusta. Organisaatio arvioi näiden sopimusten ja velvoitteiden toteutumista ennakolta suunnitellulla tavalla.

   - sopimuksen tulee sisältää toimintamallit tietoturvallisuuden, tietosuojan, toiminnan jatkuvuuden ja varautumisen prosessien osalta
   - organisaatio on (rekisterinpitäjänä) päävastuussa siitä, että tietojen käsittely on yleisen tietosuoja-asetuksen mukaista
   - organisaatiolla tulee olla ohjeistus henkilöstölle ja palvelutoimittajille eri tasoille luokiteltujen tietoaineistojen käsittelystä

6. Organisaation johto varmistaa, että henkilöstö saa tarvittavan ohjeistuksen ja koulutuksen turvallisesta toimimisesta digitaalisessa toimintaympäristössä sekä salassa pidettävien tietojen, turvallisuusluokiteltavien (valtionhallinto) tietojen ja kaikkien henkilötietojen käsittelystä.

   Digiturvallinen elämä -verkkokoulutukset

   Digiturvallinen elämä -peli

7. Palveluiden tietoturvallisuuden ja henkilötietojen käsittelyn tilasta ja näiden kehittymisestä raportoidaan niistä vastaavalle johdolle säännöllisesti. Merkittävistä muutoksista ja uusista kriittisistä uhista tai toteutuneista riskeistä raportoidaan välittömästi ja ne otetaan käsittelyyn viipymättä.

8. Organisaatio on varmistanut, että riskilähtöiset tietoturva- ja tietosuojatoimenpiteet sekä ohjeistukset on rakennettu osaksi sen kehitysmalleja, kuten kokonaisarkkitehtuuria, projektinhallintamallia sekä järjestelmäkehitysmallia.

9. Organisaatio on varmistanut, että riskien perusteella tietoturvan ja tietosuojan toteuttamiseen on kiinnitetty vuotuisesti riittävästi resursseja, kuten ammattitaitoista henkilöstöä, rahallista budjettia ja teknisiä tietoturvapalveluita.

Viranomaisohjeita

Digi- ja väestötietoviraston ohjeita:

Kysymyksiä ja vastauksia identiteettivarkauden tai tietovuodon uhrille

Liikenne- ja viestintäviraston ohjeita:

Oppaat organisaatioille ja yrityksille

Esimerkiksi:

Näin suojaudut tietomurroilta

Kyberturvallisuus ja yrityksen hallituksen vastuu -opas

Pienyritysten kyberturvallisuusopas

Tietosuojavaltuutetun toimiston ohjeita:

Ohjeet organisaatioille henkilötietojen käsittelyssä

Esimerkiksi:

Henkilötietojen käsittely

Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi

Tietoturvaloukkaukset

Usein kysyttyä