4.4.2022

Tietoturva- ja tietosuojaraportti vuodelta 2021

EU:n yleinen tietosuoja-asetus (2016/679), joka tuli voimaan 25.5.2018, asettaa tiettyjä velvollisuuksia rekisterinpitäjälle. Tässä raportissa käydään läpi tietosuojan ja tietoturvan kannalta keskeisimmät tapahtumat.

Arkisto ja asianhallinta

Vuoden 2021 aikana valmisteltiin Dynasty 10 –järjestelmän käyttöönottoa. Käyttöönoton yhteydessä laadittiin kuntayhtymälle myös tiedonohjaussuunnitelma (TOS). Dynasty 10 -järjestelmän käyttöönotto oli 1.1.2022. TOSin sisältöä tullaan päivittämään jatkuvasti vastaamaan käytänteitä.

Vuoden 2021 aikana muutettiin kuntayhtymän yleisen postilaatikon (jedu@jedu.fi) lukuoikeuksia niin, että vain johdon sihteeri ja kirjaamo saavat lukea viestejä. Viestit lähetetään vain oikeille henkilöille. Aikaisemmin viestin sai koko esimiesfoorumi, jolloin viesteissä olevat arkaluonteisetkin asiat pääsivät liian ison lukijajoukon nähtäville.

Tietosuoja

Henkilöstön käytössä olevien kannettavien tietokoneiden kiintolevyjen sisältö on salattu Bitlocker-salauksella, mikä estää kiintolevyllä olevien tietojen joutumisen vääriin käsiin esim. tilanteessa, jossa tietokone varastetaan. Bitlockerin palautusavaimet (recovery key) on siirretty vanhentuvalta paikalliselta hallintapalvelimelta Microsoftin pilvipohjaiseen Azure active directoryyn

Tietohallinnon intran sivuilta löytyy tietoturvasta ja tietosuojasta omat osionsa. Lisäksi henkilöstöltä vaaditaan suorittamaan omatoiminen tietosuojakoulutus, joka on Tietosuojan ABC julkishallinnon henkilöstölle. Koulutuksen käytyä henkilö rekisteröi suorituksen koulutusrekisteriin. Näin pyritään täyttämään osaltaan tietosuoja-asetuksen vaatimus osoitettavuudesta. Tällä on tarkoitus pystyä osoittamaan se, että henkilöstöä on koulutettu.

Henkilöstölle on kerrottu tietosuojaan ja tietoturvaan liittyvistä pelisäännöistä henkilöstökoulutuspäivissä sekä eri paikkakuntien henkilöstökokouksissa. Lisäksi tilaisuuksissa on muistutettu tietosuojakoulutuksen tekemisestä ja testistä.

Vuoden 2021 aikana on henkilöstöstä rekisteröinyt testin suorituksen vain 98 henkilöä. Testin tekemistä on yritetty viedä lähiesimiesten kautta henkilöstölle

mutta tuloksetta. Tavoitteena on, että vuoden 2022 aikana jokainen henkilöstöön kuuluva suorittaa testin.

Tietosuojan kannalta on erittäin hankalaa henkilöstön omat rekisterit, joita ovat esimerkiksi opettajan kalenterissa olevat tiedot. Opettajan tavarat saattavat jäädä vartioimatta avoimeen luokkaan, jolloin tietosuojan kannalta tiedot voivat helposti joutua vääriin käsiin. Info- ja koulutustilaisuuksissa on tuotu useamman kerran esille, että tällaisten tietojen säilytyksessä pitää noudattaa erityistä huolellisuutta.

Videovalvonnan tietosuojaseloste on tehty ja hyväksytty YT-toimikunnassa. Videovalvonnan tietosuojaseloste on julkaistu kuntayhtymän www-sivuilla.

Vuoden 2021 aikana on otettu testikäyttöön uuden henkilön oikeuksien ja tunnuksien luomiseen liittyvä työnkulku. Työnkulun kautta esimies määrittelee, mitä oikeuksia ja tunnuksia uusi työntekijä tarvitsee. Työnkulkua tullaan kehittämään vuoden 2022 aikana ja tarkoituksena on ulottaa se myös oikeuksien muutoksiin ja henkilön työsuhteen loppumiseen.

Sähköpostin automaattinen salaaminen tapahtuu postijärjestelmän ylläpitäjän määrittämiin sääntöihin perustuen, jolloin viestin sisällöstä etsitään tiettyjä tuntomerkkejä ja niiden löydyttyä järjestelmä salaa viestin automaattisesti. Tällä hetkellä viesti salataan automaattisesti, kun se täyttää seuraavat ehdot:

- Vastaanottaja on kuntayhtymän ulkopuolinen henkilö eli osoitteen loppuosa ei ole @jedu.fi tai @student.jedu.fi
- Viesti sisältää sosiaaliturvatunnuksen tai –tunnuksia joko itse viestiin kirjoitettuna tai esim. Excel-, Word, tai pdf-liitetiedostossa

Ulospäin lähetettävä sähköposti voidaan salata myös lisäämällä viestin aihe-kentään teksti [salaus].

Tietoturva

Kuntayhtymässä otettiin käyttöön vuoden 2021 aikana Microsoftin Defender –tietoturvaohjelmisto työasemien osalta. Defenderin käyttöä laajennettiin vuoden 2022 alussa koskemaan myös kuntayhtymän hallinnassa olevia palvelimia. Ohjelmisto hoitaa työasemien virustorjunnan, haavoittuvuustarkistuksen sekä endpoint detection and responsen. Näillä työkaluilla hoidetaan suojausta kyberuhkia vastaan.

Microsoft Defenderin ASR (attack surface reduction) -säännöt on käytössä kaikilla työasemilla. Näillä estetään tyypillisimpien hyökkäystapojen käyttämiä toimintoja.

Lisäksi on otettu muita Defenderin suosittelemia tietoturvaa parantavien asetuksia työasemille, koskien esim. seuraavia asetuksia

- LM ja NTLM
- verkon selaaminen kirjautumatta
- WinRM Basic-autentikointi

Havaittiin ongelmia Google Chrome -selaimen automaattipäivityksen osalta. Asennettuja versioita on alettu seuraamaan tarkemmin haavoittuvuustarkkailulla ja tarvittaessa laitettu uusi versio SCCM:n avulla kaikille koneille kerralla.

Työasemissa todettiin olevan vanhentuneita, tuen ulkopuolelle jääneitä Windows 10 -versioita. Tilannetta korjattu versiopäivityksillä.

Kuntayhtymän verkon ulkopuolella käytettävien koneiden hallinnassa pitämistä helpotettu Always On VPN -ratkaisun avulla, jolloin koneet keskustelevat SCCM-palvelimelle myös muualla ollessaan ja sitä kautta myös Intune-hallintaan.

Vanhentuneiden Adobe Creative Cloud -paketit on korvattu tuen piirissä olevilla sekä on otettu käyttöön tietoturvapäivitysten asennusten automatisointi Adobe Update Server Setup Tool -palvelimelta

Työasemien Windows-palomuurien hallinta on siirretty AD:n ryhmäkäytännöistä Intuneen.

Kuntayhtymä on mukana DigiTyy – DIGIturvallinen Työkulttuuri ja Ympäristö -hankkeessa. Hanke on Kalajoen kaupungin sekä 18 muun hakijaorganisaation yhteishanke digitaalisen turvallisuuden prosessien ja hallintamallien kehittämiseksi.

Digityy-hankkeen viitekehys pitää sisällään tietosuojan, tietoturvallisuuden, toiminnan jatkuvuuden hallinnan ja varautumisen sekä riskien hallinnan. Digiturvaryhmän tarkoituksena on edistää yhteistyön avulla kuntien ja kuntayhtymien lakisääteisiä velvollisuuksia digitaalisen turvallisuuden osalta.

Poikkeamat

Vuoden aikana merkittävin ja toimintaa haittaava tekijä oli Wilmaan kohdistuva palvelunestohyökkäys. Wilma on siirtynyt vuoden 2020 aikana pilvipalveluun ja palvelunestohyökkäys kohdistui tällöin hyvin moneen koulutuksenjärjestäjään. Visma sai järjestelmänsä kuntoon muutaman päivän aikana ja Visma vahvisti ja varmensi järjestelmiään tulevaisuuden varalle, jottei tällaista pääsisi käymään.

Yksi opiskelijatietokone oli vuoden aikana hetken aikaa hukassa, mutta selvittelyjen jälkeen tällekin löytyi ratkaisu ja ei aiheuttanut tietosuojan tai tietoturvan kannalta ongelmaa.

Vuonna 2021 oli paljon erilaisia tietojenkalasteluyrityksia maailmalaajuisesti. Tietohallinto on tiedottanut intran uutisissa aina tällaisista uhkista ja tiedossa ei ole näiden osalta mitään erityisiä ongelmia. Tietojenkalasteluyrityksiä vastaan

suojaudutaan käyttämällä kaksivaiheista tunnistautumista kuntayhtymän verkkopalveluissa henkilöstön osalta sekä painottamalla perehdytysten yhteydessä turvallista tapaa tunnusten ja salasanojen kanssa toimimiseen.

Yhteenveto

Tietosuojan ABC-koulutus julkishallinnon henkilöstölle on velvoitettava henkilöstölle pakolliseksi koulutukseksi.

Luottamushenkilöille on tehtävä oma tietopaketti tietosuojasta ja tietoturvasta.

Viranhaltijan, työntekijän ja luottamushenkilön, jotka käsittelevät tai saavat henkilötietoja työtään tai päätöksentekoa varten, tulee huomioida henkilötietojen tietosuojavaatimukset.

Työntekijän oikeuksien ja tunnusten määrittelemiseen on tehtävä prosessikuvaus, missä määritellään, kuinka asiat kuntayhtymässä tehdään.

Kuntayhtymälle on luotava kyber-, tieturva- ja tietosuojastrategiat. Osaltaan DigiTyy-hanke auttaa näiden tekemisessä.

On tehtävä lähitulevaisuudessa tietojärjestelmien osalta riskianalyysit sekä toipumissuunnitelmat hyökkäyksiltä.

Tietotilinpäätös tehdään kevään 2022 aikana.

Kuntayhtymän johtoryhmän säännölliset tietoturva- ja tietosuojakatsaukset aloitetaan vuonna 2022.

Henkilöstöä on koulutettava ja meneillään olevista hyökkäys- tai kalastelukampanjoista tiedotettava akuutissa vaiheessa.

Arto Veikkola

Tietohallintopäällikkö