Ari Itkonen, BDO Oy
11.11.2020

K 9/2020 vp - Eduskunnan tilintarkastajien tilintarkastuskertomus eduskunnan tilinpäätöksestä, toimintakertomuksesta ja kirjanpidosta sekä hallinnosta vuodelta 2019 / Asiantuntijapyyntö

Tarkastusvaliokunta torstai 12.11.2020 klo 12.30

Eduskunta, tietoturvan hallinnon tarkastus

Tarkastus toteutettiin vuoden 2019 tilintarkastuksen yhteydessä. Arvioinnin kohteena oli eduskunnan tietoturvan hallinnointi. Auditoinnin tarkoituksena oli kartoittaa tietoturvan hallinnointimenettelyt ja arvioida niiden riittävyys huomioiden toiminnan laajuus, käsiteltävät tiedot ja toimintaan liittyvät vaatimukset. Tarkastus kohdistui tietoturvan hallinnon prosesseihin, ohjeistukseen ja toimivuuteen koko organisaation tasolla. Tarkastus ei sisältänyt yksittäisten kontrollien todentamista eikä järjestelmien ja alihankkijoiden tietoturvan verifiointia.

Tietoturvan hallinnan tilan arvioitiin olevan *pääsääntöisesti hyvällä tai toimivalla* tasolla. Jäljessä esitetään tarkastuksen keskeiset kehittämistä edellyttävät havainnot ja suositukset.

Tilintarkastajien kokouksessa 11.11.2020 tietoturvavastaavalta saadun tiedon mukaan suositukset on huomioitu ja suosituksia edistetään. Toimenpiteiden käynnistäminen odottaa osittain eduskunnan normaaliin toimintaan siirtymistä.

Tietoturvariskien hallinta ja strateginen suunnittelu

Tietohallinnolla ja tietoturvalla on yhteinen riskienhallintasuunnitelma. Kanslian muut osastot tekevät oman riskienhallintasuunnitelman itsenäisesti. Yhteistyötä muiden osastojen kanssa on vähän, vaikka yleensä tietohallinnon ja tietoturvan riskit koskettavat koko organisaatiota ja riskien omistajat ovat tietohallinnon ulkopuolella.

Riskinä on, että riskien hallinta siiloutuu, eikä riskejä hallita kokonaisuutena ja kriisitilanteissa eri osastojen toiminnan koordinointi on puutteellista.

Suosittelemme, että riskienhallinnassa

- Lisätään yhteistyötä eri osastojen välillä,
- Tietoturvariskit kerätään koko organisaatiolta,
- Riskien omistajat osallistuvat tietoturvariskien vakavuuden arviointiin.

Tietoturvan organisointi

Tietoturvalla ei ole ohjausryhmää.

Riskinä on, että toimintaa ei ohjata ja kehitetä riittävän kokonaisvaltaisesti ja eduskunnan toiminnan vaatimusten mukaisesti.

Suosittelemme, että perustetaan tietoturvan ohjausryhmä, joka

- kokoontuu säännöllisesti, pitää kokouksista pöytäkirjaa ja
- käsittelee mm. tietoturvapoikkeamat, uhat/riskit, kehitystoimenpiteet ja vuosikellossa erikseen määritellyt tehtävät.

Omaisuuden tietoturva (tieto, prosessit, järjestelmät, laitteet)

Tarkastushetkellä selvitettiin dokumenttien tallennusta pilvipalveluihin. Pilvipalveluihin voidaan tallentaa sekä sisäiseksi että julkiseksi määritettyä materiaalia, ja sieltä voidaan jakaa materiaalia myös organisaation ulkopuolelle. Pilviratkaisu voidaan nähdä kokonaisuutena, jonka hallinnointiin liittyy erilaisia riskejä.

Riskinä on, että pilvipalvelussa käsiteltävien dokumenttien tietoturva vaarantuu.

Suosittelemme, että

- vertaillaan erilaisia ratkaisumalleja (esim. nykyinen, pilviratkaisu, hybridi),
- tehdään huolellinen ja perusteellinen riskiarvio, jonka tiedon omistajan tulee ymmärtää ja hyväksyä,
- määritellään ja tiedotetaan pilvipalveluympäristön loppukäyttäjän ohjeet.

Toiminnan jatkuvuuden hallinta

Eduskunnan toiminnalle kriittiset tietojenkäsittelyjärjestelmät on tunnistettu, ja niille on laadittu tietojärjestelmien toipumissuunnitelmat. Jatkuvuussuunnitelmia ei ollut laadittu normaaliolojen vakavien häiriöiden varalta. Saadun tiedon mukaan eduskunnassa on keskitytty varautumaan hallinnollisin ja teknisin keinoin erilaisiin vakaviin häiriötilanteisiin.

Harjoitusten perusteella on kirjattu varautumismenettelyjen sekä tulevien harjoitusten kehitystarpeita.

Mahdolliset puutteet jatkuvuussuunnitelmissa ja toipumissuunnitelmissa voivat vaikuttaa eduskunnan tukitoimintojen palvelukykyyn.

Suosittelemme:

- laatimaan tärkeille (hallinnollisille) toiminnoille jatkuvuussuunnitelmat, joissa on huomioitu normaaliolojen vakavat häiriötilanteet esim. tulipalo-, savu-, kosteusvahingot ja sairausepidemiat,
- testaamaan kriittisiin tietojärjestelmiin liittyvät toipumissuunnitelmat sekä varmistamaan niiden yhteensopivuuden jatkuvuussuunnitelmien kanssa.

Poikkeustilanteisiin varautuminen

Haastatteluissa ilmeni, että ulkoisten palvelutoimittajien toiminnan jatkuvuuden varmistaminen ja erityisesti keskeisten henkilöresurssien varmistaminen poikkeuksellisissa oloissa oli tunnistettu selvitettäväksi ja varmistettavaksi asiaksi. Sopimuksissa edellytetään palvelutoimittajilta riittävää resurssointia.

Suosittelemme selvittämään ja varmistamaan palvelutoimittajien riittävät henkilöresurssit myös poikkeusoloissa.