

Digitaalisen turvallisuuden muistilista kuntajohtajalle

Elisa Kettunen, kehittämispäällikkö ja ratkaisupäällikkö

elisa.kettunen@kuntaliitto.fi

Digitaalisen turvallisuuden muistilista kuntajohtajalle

KYSY ITSELTÄSI, ONKO KUNNASSA:

KYLLÄ!

EI TAI EN TIEDÄ

REALISTINEN TILANNEKUVA – VAHVUUDET JA HEIKKOUEDET. Onko kunnassa ajantasainen tilannekuva kokonaisturvallisuudesta ja sen osana digitaalisesta turvallisuudesta? Huomioiden henkilöstö, ohjelmistot, infrastruktuuri, viestintä ja kumppanuudet? Mitä tietoa käytämme ja ylläpidämme ja millaisten palveluiden jatkuvuus täytyy kyetä aina varmistamaan?

Hienoa! Muistattehan myös ylläpitää tilannekuvaa koko ajan ja varmistaa että tilannekuva on jaettu henkilöstön kanssa. Uhkaskenaarioiden tunnistaminen erilaisten tilanteiden säännöllinen harjoittelu on myös tärkeää.

Tutustu keskeiseen lainsäädäntöön, kuten tiedonhallintalakiin ja ryhdy ottamaan tilannetta haltuun! Tilannekuvan täytyy myös muuttua teoiksi ja tavoitteelliseksi toiminnaksi. Ota avuksi asiantuntijoita eri toimialoilta, myös ulkopuolista osaamista voi hyödyntää.

ROOLIT JA VASTUUT. Onko kunnassa määritelty vastuut tietoturvaan ja kyberturvallisuuteen liittyen, ymmärtävätkö nimetyt henkilöt vastuunsa?

Loistavaa! Kannattaa keskustella vastuuhenkilöiden kanssa säännöllisesti heidän vastuistaan ja mahdollisista uusista velvoitteista tai haasteista. Säännöllinen keskustelu auttaa myös kuntajohtajaa ylläpitämään tilannekuvaa ja valmistautumaan.

Vastuut on tärkeä tunnistaa ja määritellä. Erityisesti muutostilanteissa, kuten henkilöiden vaihtuessa tai sopimuksia uusittaessa. Kunta on laaja kokonaisuus, kannattaa huomioida eri toimialojen erityispiirteet.

RESURSSIT. Ovatko vastuuhenkilöt resursoitu riittävästi, tarvitsevatko he koulutusta, vertaisverkostojen tukea tai rahaa, jotta voivat hoitaa tehtävänsä hyvin?

On tärkeää, että resursseja kohdennetaan digitaaliseen turvallisuuteen ja sen kehittämiseen – **erinomaista** jos tämä on teillä ymmärretty! Myös henkilöstön osaamisen kehittäminen ja ylläpitäminen on tärkeää.

Tietoturva on kuin vakuutus, se voi tuntua kalliilta, mutta vielä kalliimmaksi se voi tulla jos sitä ei ole. **Etsi tueksesi kollegoiden ja asiantuntijoiden näkemyksiä, mihin ja miten resursseja kannattaisi kohdentaa.** Digitaalisesta turvallisuudesta huolehtiminen on tietoyhteiskunnan varautumistaitoja ja suojelee arkeamme.

TOIMINTA POIKKEAVASSA TILANTEESSA. Onko kunnassa selvää, mistä voi saada apua jos sitä tarvitaan? Apua voidaan tarvita nopeasti, eli ovatko numerot selvillä ja esim. sopimukset kunnossa. Kuinka toimitaan, jos tilanne sattuu virka-ajan ulkopuolella? Osataanko toimia tarvittaessa myös analogisesti, eli tilanteessa jossa normaalisti käytössä olevat digitaaliset järjestelmät eivät ole käytössä?

Hädän hetkellä ystävää tunnetaan! On tärkeää, että riskeihin on varauduttu ja tunnistettu, missä kulkevat oman osaamisen ja resurssien rajat. Kumppaneiden kanssa kannattaa säännöllisesti päivittää tilannekuva, jotta äkillisessä tilanteessa yhteistyö sujuu saumattomasti. Poikkeavassa tilanteessa on tärkeää varmistaa, että henkilöstö ja kuntalaiset saavat oikeaa informaatiota tilanteesta, nopeasti.

Kunta vastaa itse omasta digitaalisesta turvallisuudestaan. Aina oma osaaminen ei riitä ja myös näiden tilanteiden varalle kunnalla on hyvä olla suunnitelma B. Tämä suunnitelma kannattaa tehdä silloin, kun mitään hätää ei ole. Hädän hetkellä ei ehdi suunnitella ja se tulee kalliiksi sekä inhimillisesti että euroissa.

KUNTA
LIITTO

Mistä kunta voi saada apua digitaalisen turvallisuuden alueella?

Verkostot

- Kuntakentän tietoturvavastaavien verkosto
- Kuntien tietosuojavastaavien verkosto
- Turvallinen ja kriisinkestävä kunta
- AKUSTI (Alueiden ja kuntien sosiaali- ja terveydenhuollon tietohallintoyhteistyöfoorumi), Kuntaliitto.
- Kunnan ja asiantuntijoiden omat yhteistyöverkostot

Viranomaiset

A) Akuutti tilanne:

Poliisi

Tietosuojavaltuutetun toimisto

Kyberturvallisuuskeskus

B) Ennakointi

Digi- ja väestötietovirasto: www.dvv.fi

Huoltovarmuuskeskus

Kunnan omat kumppanit (yrityksiä)

Digitaalisen turvallisuuden käsite

- Digitaaliseen turvallisuuteen kuuluvat *riskien hallinta ja käsittely, toiminnan jatkuvuuden hallinta ja varautuminen, tietoturvallisuus ja tietosuoja sekä kyberturvallisuus.*
- *Kyberturvallisuudella* tarkoitetaan digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.
- [Lisätietoa Kuntaliiton sivuilta.](#)
- Käsitteen lähde: [Julkisen hallinnon digitaalinen turvallisuus](#) –julkaisu valtiovarainministeriö.

