Turvallisuustieto Oy, Tampere
Toimitusjohtaja Pentti Harmanen:

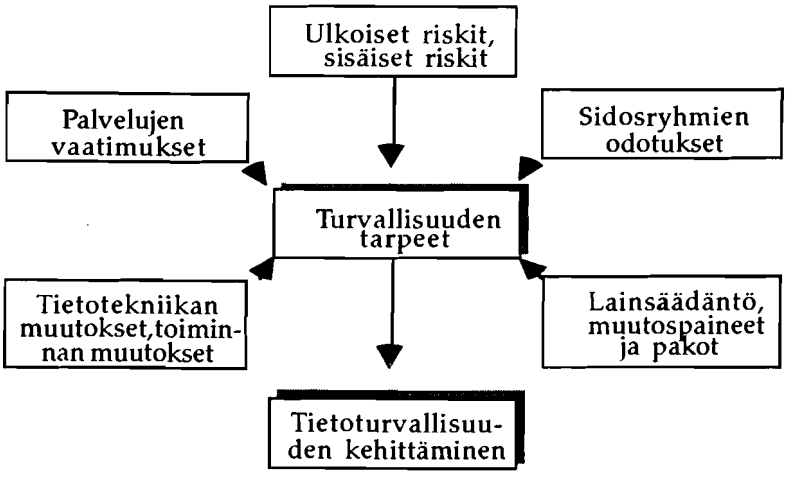
TIETOJENKÄSITTELYN TURVALLISUUS KUNNALLISHALLINNOSSA

1. Johdanto

Tietojenkäsittelyn merkitys yritysten, laitosten ja koko yhteiskunnan toimivuudelle on nykypäivänä ratkaisevan tärkeä. Riippuvuus tietojenkäsittelystä ei ole kasvanut vain yritysten ja laitosten sisällä, vaan myös niiden välillä. Tietojenkäsittelyn hajautuminen, tietoliikenteen hyödyntäminen sekä yhä laajeneva atk-palvelujen hyväksikäyttö lisäävät riippuvuutta tietojenkäsittelystä ja sen turvallisuudelle asetettavia vaatimuksia. Lähes kaikki yhteiskunnan tärkeimmät toiminnot ovat tietotekniikasta riippuvia. Tietotekniikasta on tullut strateginen resurssi myös kunnille sekä kuntayhtymille. Jotta vaatimukset tietojen oikeellisuudelle ja ajankohtaisuudelle voitaisiin täyttää, on tietojärjestelmien toimittava häiriöittä. Tiedon on oltava virheetöntä myös tärkeiden päätösten perustaksi. Tietoturvallisuuden perustana on oltava tietotekniikasta riippuvien toimintojen ja palvelujen tarpeet ja tietojenkäsittelyn merkitys tärkeimpien ja välttämättömien tehtävien hoidossa sekä käsitys toimintaa uhkaavista riskeistä.

2. Tietojenkäsittelyn haavoittuvuus

Haavoittuvuudella mitataan tavallisesti arkuutta atk-toiminnan häiriöille, tietotekniikan keskeytymiselle tai vioittumiselle sekä virheille ja väärinkäytöksille. Vaikka tietojärjestelmässä yksittäisten osien turvallisuusvaatimukset vaihtelevat, tulee koko järjestelmän perusturvallisuuden olla tasolla, joka täyttää toiminnan kannalta kattavasti käytettävyys-, tiedon suojaus-, eheys- ja salassapitovaatimukset. Haavoittuvassa tietojenkäsittelyssä riskien seurauksena saattavat olla virheet tiedoissa, puutteelliset tulosteet, menetetyt tiedot, päätösten viivästyminen, lisääntyneet kustannukset, jatkuvista häiriöistä aiheutuva tyytymättömyys, työilmaston huononeminen, julkisuuskuvamenetykset, muille aiheutuneet vahingot, sanktiot, koko toiminnan estyminen tai toiminnan jatkamisen kannalta kriittiset menetykset.



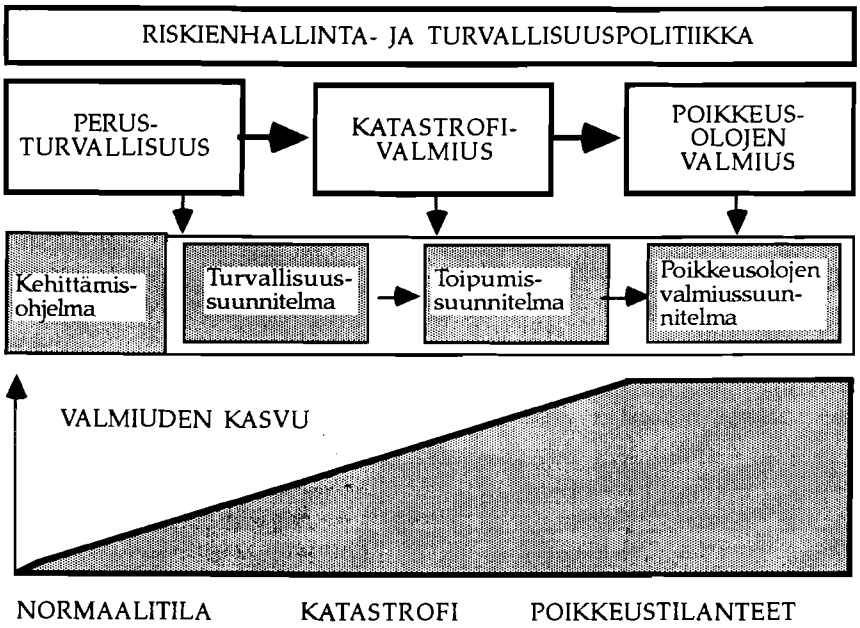
Valtaosa tietojenkäsittelyyn kohdistuvista riskeistä on tavanomaisia käyttövirheitä, teknisiä vikoja, häiriöitä, ohjelmavirheitä ja tiedostojen tuhoutumisia. Pääosa riskeistä on

sisäisiä, toisin kuin yleisesti luullaan. Nykyaikaisessa avoimessa tietojenkäsittelyssä korostuvat myös ulkoiset uhkatekijät.

3. Tietojenkäsittelyn turvallisuus

Tietojenkäsittelyn turvallisuus jaetaan usein toimenpiteiden luonteen perusteella karkeasti
- fyysiseen turvallisuuteen,
- loogiseen turvallisuuteen sekä
- tiedonsiirron suojaamiseen.

Tietojenkäsittelyn turvallisuussuunnittelun kokonaistavoitteena on
- perusturvallisuuden luominen tietojenkäsittelyyn liittyvien vahinkojen, väärinkäytösten ja häiriöiden välttämiseksi
- varautuminen katastrofitilanteiden aiheuttamien vahinkojen rajoittamiseen sekä
- valmiuden luominen toiminnalle poikkeusoloissa.



Tietojenkäsittelyn yleisesti tunnetut heikot kohdat - fyysiset riskit ja tietoriskit - tulevat vastaan yhä useammin. Näihin riskitekijöihin varautuminen on tietojenkäsittelyn perusturvallisuutta, toiminnan varmistamista normaalioloissa. Atk-järjestelmän vioittuminen tai tuhoutuminen voi johtaa vahvasti atk-riippuvan organisaation vaikeisiin ongelmiin. Toiminnan jatkaminen edellyttää valmiutta katastrofitilanteiden hallintaan. Valmius luodaan toipumissuunnitelmin. Kriisitilanteissa keskeisen atk-toiminnan lamautuminen aiheuttaisi yhteiskunnalle suuria vaikeuksia peruselinehtojen ylläpitämisessä, sillä harvoin enää kyetään toimimaan manuaalisten menetelmien varassa tai siirtymään sellaisiin laajamittaisesti. Toimenpiteet sisältyvät poikkeusolojen atk-valmiussuunnitelmaan. Suunnitteluvelvoite on valmiuslakiin perustuva.

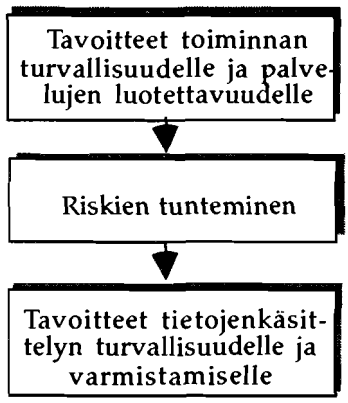
Tietojenkäsittelyn turvaaminen muodostaa yhtenäisen valmiussuunnitelman perusturvallisuudesta katastrofivalmiuden kautta poikkeusolojen valmiuteen.

Tietojenkäsittelyn turvaamiseen käytettävät keinot eivät ole vain tietoteknisiä. Tavanomaisen turvallisuustoiminnan keinoin luodut puitteet ja turvattu ympäristö ovat tärkeimpiä atk-toiminnan perusedellytyksiä.

Tietoturvallisuus kohdistuu koko tietojenkäsittelyyn, myös manuaaliseen käsittelyyn ennen atk-käsittelyä, sen aikana ja sen jälkeen. Hajautetussa tietojenkäsittelyssä on turvallisuustoimenpitein suojattava käyttöympäristö lukuisissa eri työpisteissä.

3.1. Vastuu tietoturvallisuudesta

Vastuuta tietoturvallisuustoimenpiteistä on tarkasteltava toiminnan ja palvelujen näkökulmasta. Johtamistavan muuttuminen, vastuun hajauttaminen tulosyksiköihin ja tietotekniikan muutos ovat tulosvastuun ohella ohjanneet tietotekniikan käytön ja sen suunnittelun muiden kuin tietotekniikan ammattilaisten tehtäväksi. Samoin on käynyt myös turvallisuudessa. Atk-henkilöstö ei voi riittävän läheltä nähdä eri hallintokunnissa ja yksiköissä palveluille ja toiminnoille asetettavia vaatimuksia. Ilman käyttäjän osallistumista turvallisuuden määrittelyyn voi toimintaan kätkeytyä riskejä, joista kukaan ei ota vastuuta.



Usein ajatellaan, että tietoturvallisuudesta päättävän johdon tulisi tuntea yksityiskohtaisesti turvallisuustoimenpiteet. Tämä ei ole tarpeellista. Varsinaisen toiminnan tuntevalla johdolla ja esimiehillä on parhaat edellytykset asettaa vaatimukset palvelujen turvaamiselle.

3.2. Turvallisuusvaatimukset

Yleiset käyttövaatimukset edellyttävät, että

- *käytettävyys* tietojärjestelmissä sallii käyttäjien keskeytymättä hyödyntää tietojärjestelmien toimintoja
- järjestelmien tuottaman informaation *tietosisältö* on laadultaan odotusten mukaista; oikeaa ja ajankohtaista
- tietojenkäsittely on *fyysisesti suojattu käytön* kannalta ja järjestelmässä voidaan suojata tiedot ja ohjelmistot tahattomalta, luvattomalta tai tahalliselta tuhoamiselta, menetykseltä, käyttämiseltä ja muuttamiselta
- järjestelmien *toimivuus* on hyvä
- tapahtumien *tarkastettavuus* säilyy
- *lähiverkko* on turvallinen ja varmistettu
- *lainsäädännön vaatimukset* täyttyvät

- *arkistoitavuus* varmistetaan ja
- *turvallisuusuunnitelmat* ovat olemassa.

Elintärkeän tietojenkäsittelyn varmistaminen ja turvallisuusuunnittelu edellyttävät lisäksi
- *tietojärjestelmien tärkeysluokitusta*
- *tietoliikenteen tärkeysluokitusta ja*
- *tiedon salassapitoluokitusta.*

Erityinen huomio hallintoyksikön tietojenkäsittelyssä on kohdistettava lähiverkon turvallisuuden luomiseen ja ylläpitämiseen, sillä lähiverkko on ja tulee pitkään olemaan koko tietojenkäsittelyn ja tiedonsiirron perusrunko. Verkossa on siten oltava oltava selkeät turvallisuusperiaatteet pääsyoikeuksille ja liittymille, käytölle, tiedonsiirrolle ja varmistuksille. Erityisesti OVT:ssä (organisaatioiden välinen tietoliikenne) on turvallisuuden merkitys suuri mm. lähetteiden tutkimustulosten siirrossa sairaaloiden ja laboratorioiden välillä, tilausten ja laskujen siirrossa taloushallinnossa sekä erilaisten henkilö- ym. rekistereiden päivityksessä, joihin OVT hyvin sopii.

3.3. Turvallisuustoimenpiteet

Sekä turvallisuuden vuoksi että taloudellisesti on järkevää suunnitella turvallisuustoimenpiteet jo tietojärjestelmää hankittaessa, järjestelmäkehityksessä ja toimintaympäristöä rakennettaessa. Myöhemmin niiden tekeminen on jo vaikeampaa, joskus jopa mahdotontakin.

Turvallisuustoimenpiteiden perusteiksi selvitetään
- elintärkeät toiminnat ja palvelut
- niiden riippuvuus tietojenkäsittelystä
- keskeisimmät atk-toiminnan tekijät, joiden turvaamiseen ja varmistamiseen turvallisuustoimenpiteet kohdistetaan
- suojattava tiedot
- laatuvaatimukset
- käytettävyysvaatimukset
- salassapito ja tietojen suojaustarpeet ja
- varajärjestelmätarpeet.

4. Toimintaperiaatteet, organisaatio ja vastuut

Tietoturvallisuuden toimintaperiaatteiden tulee olla määriteltyjä. Ne ilmaisevat johdon tahdon ja näkemyksen turvallisuudesta ja osoittavat suunnan turvallisuuden kehittämiselle. Johdon tulee osoittaa esimiesten vastuu oman yksikkönsä toimintansa varmistamisesta. Hallintokunnissa johdolla ja järjestelmien omistajilla on vastuu oman toimintonsa tietoturvallisuusvaatimuksista ja niiden toteuttamisesta.

Kullakin tietojärjestelmällä tulee olla haltija. Tietojärjestelmän haltija on se nimetty yksikkö, joka ensisijaisesti käyttää sovellusta palveluissaan tai jota järjestelmä ensisijaisesti palvelee. Haltija vastaa järjestelmän toimintavarmuudesta oman toiminnan sekä tietojärjestelmästä riippuvien muiden toimintojen varmistamiseksi.

Jokaisen atk-käyttäjän velvollisuutena on tuntea sekä yleiset että omaa tehtäväänsä koskevat erikoisohjeet tietoturvallisuudesta ja noudattaa niitä. Käyttäjän tulee tuntea menettelyt myös puutteiden raportoinnista.

Palveluyrityksessä ei yleensä ole mahdollista seurata muutoksia kunnan ja järjestelmän haltijan toiminnassa. Siksi ostettuja atk-palveluja toiminnassaan käyttävä hallintoyksikkö asettaa atk-palvelutalon ja sen atk-käytön turvalli-suudelle. Yhteistoiminta turvallisuuskysymyksissä on sovittava.

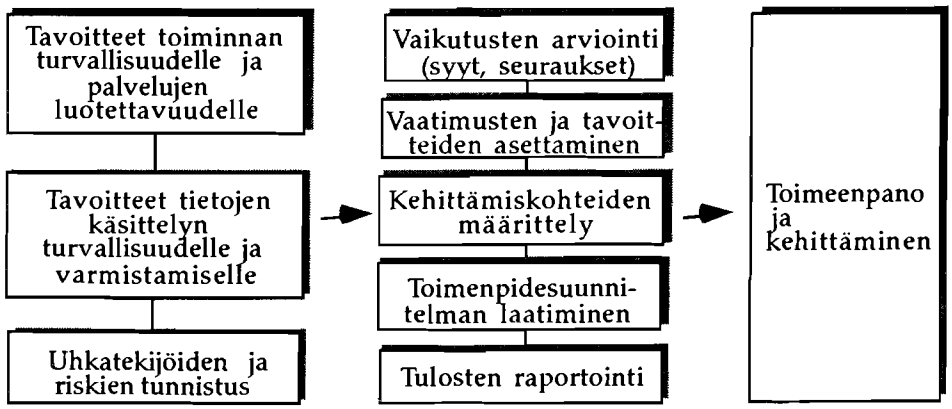
5. Tietoturvallisuustoiminnan käynnistäminen ja turvallisuusanalyysi

Tietoturvallisuusanalyysin tarkoituksena on hankkia yksityiskohtaisia tietoja tietojenkäsittelyn turvallisuudesta, riippuvuuksista ja haavoittuvuustekijöistä sekä siten parantaa vastuuhenkilöiden riskitietoisuutta ja johdon ja järjestelmien omistajien tietoja riippuvuuksien vaikutuksista toiminnassaan.

Turvallisuusanalyysissä voidaan erottaa viisi vaihetta:

- tunnistetaan tärkeimmät ja herkimmät toiminnot ja niitä tukevat atk-järjestelmät
- näille priorisoiduille tietojärjestelmille tehdään yksityiskohtaiset analyysit
- selvitetään muiden tietojärjestelmien turvallisuustarpeet ja turvallisuustoimenpiteet
- toimenpidesuunnitelmien perusteella kootaan, vastuutetaan ja käynnistetään turvallisuusprojektin suunnittelu ja toteutuksen organisointi
- toteutetaan suunnitelmat ja viedään läpi projektit

Elintärkeät tietojärjestelmät määritellään kaikissa yksiköissä. Julkishallinnossa suojattavia tietojärjestelmiä ovat mm. erilaiset henkilörekisterit. Tärkeitä ovat myös ovat sellaiset järjestelmät, joiden keskeytykset pysäyttävät laajalti asiakaspalvelun. Tiedon ja ohjelmistojen suojauksen näkökulmasta tärkeitä tietojärjestelmiä ovat maksujärjestelmät, joissa virheet voivat kertautua ja johtaa huomattaviin vahinkoihin ja luotettavuuskuvan menetykseen.



Perusturvallisuuden suunnitelma sisältää mm: johdon hyväksymät periaatteet ja turvallisuuden tavoitteet, vastuut, sijaisuudet, tietoteknisen turvallisuuden, fyysisen turvallisuuden, varmuus- ja suojakopioinnin ja kopioiden käsittelyn ja säilytyksen, valvonnan ja raportoinnin johdolle.

Toipumissuunnitelma sisältää mm. elintärkeät toiminnot, tietojärjestelmät ja sovellutukset, kuvauksen katastrofitilanteista, sallituista keskeytysajoista, varajärjestelmän, suojakopioiden ja ohjelmistosiirron, siirtosuunnitelman ja toiminnan uudelleenkäynnistyksen. Toipumisen perusedellytys on tietojenkäsittelyn dokumentointi, varmuus- ja suojakopiointi ja kopioiden käytettävyys vahinkotilanteissa.

Poikkeusolojen tietojenkäsittelyn valmiussuunnitelman päätavoite on poikkeusoloissakin välttämättömän tietojenkäsittelyn ylläpitäminen. Toimintakyvyn säilyttäminen ei ole mahdollista ilman ennalta riittävän pitkälle tehtyjä valmisteluja ja varauksia.

5.1. Turvallisuuden toteutus

Koko atk-turvallisuusajattelun lähtökohdaksi on hyvä asettaa kysymys: "Entä, jos jotain sattuu, mitä tehdään, kuka vastaa". Turvallisuussuunnittelu tapahtuu parhaiten projektina, jolle nimetään vastuuhenkilö esimerkiksi yleishallinnosta sekä työryhmä, jossa on edustettuna toiminnan ja tietojenkäsittelyn eri tahot. Johdon tulee vahvistaa hyväksymänsä vaatimukset, suunnitelmat, turvallisuuden taso ja ohjeet.

Olennaisinta tietoturvallisuuden ylläpitämisessä on turvallisuustoimenpiteiden toteutumisen, vaikutusten sekä vaatimusten noudattamisen seuranta. Merkittävistä uhkatilanteista tulee raportoida myös ylimmälle johdolle.

6. Yhdistelmä

Lisääntyvä tietotekniikkariippuvuus saattaa olla toiminnan ratkaisevan kriittinen tekijä.

Avaintekijänä koko turvallisuussuunnittelussa voidaan pitää johdon tasolla tarkistettua elintärkeiden sovellusten määrittelyä ja niiden varmistamiseksi ja suojaamiseksi käynnistettyjä toimenpiteitä.

Lopputulokselle voidaan asettaa selkeästi kaksi tavoitetta:

- tietoturvallisuuden tulee vastata varsinaisen toiminnan vaatimuksia ja
- tietoturvallisuuden on levittävä koko organisaatioon ja juurruttava käyttäjien tietoisuuteen.

Erityisesti jälkimmäinen tavoite on tärkeä niissä suurissa organisaatioissa, joissa tietojenkäsittely on hajautunut moniin pisteisiin.

Tietotekniikka ja sen turvallisuustarpeet muuttuvat nopeasti. Mikään toiminta ei pysy yllä, eikä ohjaudu ja toimi halutulla tavalla, ellei saavutettuja tuloksia seurata ja kehitetä ja toimintaa ylläpidetä. Turvallisuustoiminta ei ole tästä poikkeus.

7. Suunnittelun suuntaviivat

Atk-turvallisuussuunnittelun suuntaviivat ja toteutusperiaatteet sisältyvät Puolustustaloudellisen suunnittelukunnan ja valtiovarainministeriön järjestelyosaston julkaisuun "Tietojenkäsittelyn turvaaminen ja valmiussuunnittelu" (Valtion painatuskeskus, ISBN 951-861-629-9) ja KATKON julkaisuun "Tietojenkäsittelyn turvaaminen kunnallishallinnossa".

Tarkempia tietoja antaa Turvallisuustieto Oy, toimitusjohtaja Pentti Harmanen, puh. 931-128009.