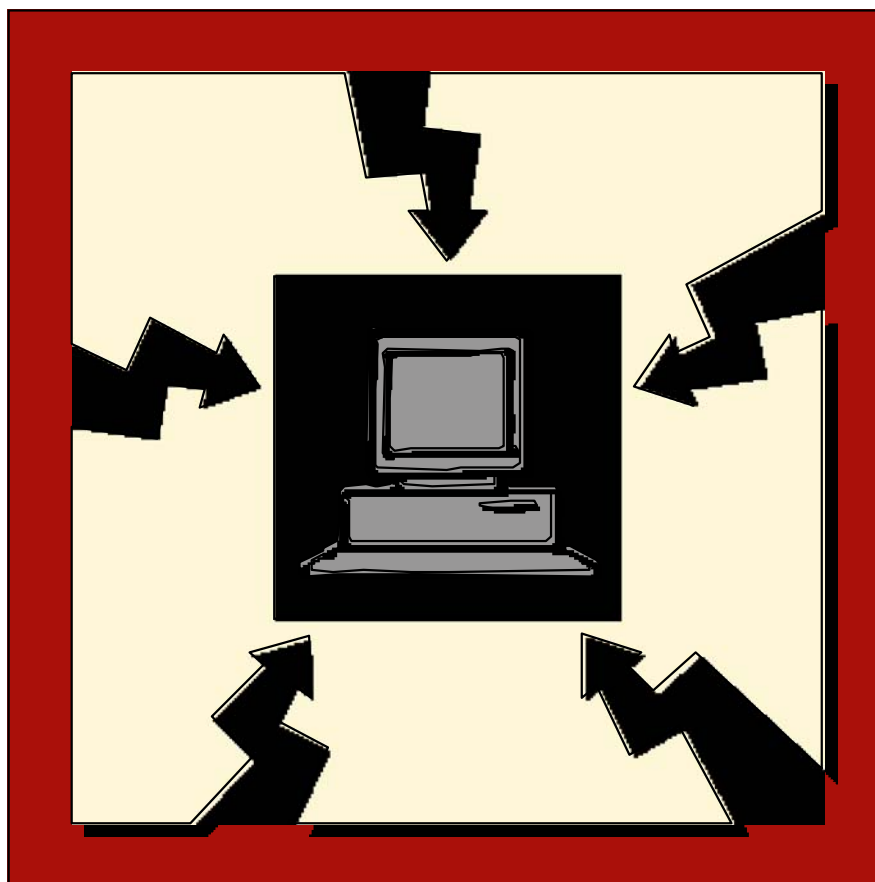




Puolustustaloudellinen suunnittelukunta



Tietotekniikan turvallisuus ja toiminnan varmistaminen

**Tietojärjestelmäjaoston ohje 1/2002
Helsinki 2002**

Tietotekniikan turvallisuus ja toiminnan varmistaminen

Puolustustaloudellinen suunnittelukunta (PTS)
Tietojärjestelmäjaosto

2002

© Puolustustaloudellinen suunnittelukunta
ISBN 951-53-2406-8
Painopaikka Domus-Offset Oy, Tampere

TIETOTEKNIIKAN TURVALLISUUS JA TOIMINNAN VARMISTAMINEN

| | |
|---|---|
| ESIPUHE | 2 |
| TIIVISTELMÄ | 2 |
| 1. JOHDANTO..... | 2 |
| 2. TOIMINNAN TURVALLISUUTEEN JA JATKUVUUTEEN VAIKUTTAVAT TEKIJÄT | 2 |
| 2.1 Lähtökohdat..... | 2 |
| 2.2 Tietoturvallisuuden yleiset tavoitteet | 2 |
| 2.3 Tietoturvallisuuden tavoitteet toiminnan näkökulmasta | 2 |
| 2.4 Normaaliolojen tietojenkäsittelyn varmistaminen..... | 2 |
| 2.5 Poikkeusolojen toiminta ja tietojenkäsittelyn varmistaminen..... | 2 |
| 2.6 Puolustustaloudellinen varautuminen..... | 2 |
| Poikkeusolot | 2 |
| Huoltovarmuus ja sen yleistavoitteet | 2 |
| Puolustustaloudellinen suunnittelu..... | 2 |
| Tietojärjestelmäalan varautuminen | 2 |
| Yritysten tärkeysluokitus..... | 2 |
| Elinkeinoelämän varautuminen ja vastuut | 2 |
| Julkishallinnon varautuminen ja vastuut | 2 |
| 3. TIETOJENKÄSITTELYN VARMISTAMINEN JOHTAMISEN OSANA..... | 2 |
| 3.1 Johtaminen ja toiminnan jatkuvuus..... | 2 |
| 3.2 Tietoturvallisuuspolitiikka..... | 2 |
| 3.3 Toiminnan suunnittelu..... | 2 |
| 3.4 Tietojärjestelmien luokitus..... | 2 |
| 3.5 Tietoturvallisuus hankinnoissa..... | 2 |
| Palvelu-, laitteisto- ja ohjelmistohankinnat | 2 |
| Järjestelmäkehitys | 2 |
| 3.6 Tietoturvallisuus ja laatu | 2 |
| 3.7 Ohjeet | 2 |
| 4. UHAT JA HAAVOITTUVUUDEN ARVIOINTI | 2 |
| 4.1 Tietotekniikan riskit sekä niiden vaikutus toimintaan..... | 2 |
| 4.2 Sisäiset ja ulkoiset uhat | 2 |
| Normaaliin toimintaan kohdistuvat uhat | 2 |
| Toiminnan jatkuvuuteen kohdistuvat uhat | 2 |
| Eriyistilanteet | 2 |
| Poikkeusolojen tietojenkäsittelyyn kohdistuvat uhat | 2 |
| 4.3 Ulkoistaminen ja turvallisuus, tietotekniikan palveluyrityksen valmius..... | 2 |
| 4.4 Sähköiset palvelut ja turvallisuus..... | 2 |
| Hyvä tiedonhallinta ja tietoturvallisuus..... | 2 |
| Internetin tietoturvallisuus..... | 2 |
| Sähköposti | 2 |
| Sähköinen kaupankäynti ja palvelujen turvallisuus | 2 |
| Salaus..... | 2 |
| Suojautuminen tietojärjestelmiin kohdistuvilta hyökkäyksiltä | 2 |
| 4.5 Tuotantojärjestelmät, palvelujärjestelmät, jatkuvat verkkopalvelut..... | 2 |
| 4.6 Haavoittuvuuden arviointi..... | 2 |
| 5. VALMIUDEN TAVOITTEET | 2 |
| 5.1 Perusturvallisuuden tavoitteet | 2 |
| Tietoturvallisuuden tavoitteet..... | 2 |
| Toipumisvalmiuden tavoitteet..... | 2 |
| 5.2 Poikkeusolojen valmiuden tavoitteet..... | 2 |

| | | |
|------|--|----|
| 6. | TIETOJENKÄSITTELYN PERUSTURVALLISUUS | 33 |
| 6.1 | Tietoturvallisuuden ja toiminnan jatkuvuuden varmistamisen perusteet | 33 |
| 6.2 | Tietoturvaluussuunnitelma | 34 |
| | Tietoturvallisuuden arviointi | 34 |
| | Tietoturvallisuuden suunnittelu | 34 |
| | Hallinnollinen tietoturvallisuus - johtaminen | 34 |
| | Henkilöstöturvallisuus | 35 |
| | Tietoaineistoturvallisuus | 35 |
| | Tietotekninen turvallisuus | 38 |
| | Fyysinen turvallisuus | 41 |
| | Valvonta | 42 |
| 6.3 | Toipumissuunnitelma | 44 |
| | Toipumisvalmiuden arviointi | 45 |
| | Toipumisvalmiuden suunnittelu | 45 |
| | Tiedostojen varmistaminen | 45 |
| | Varajärjestelmä | 46 |
| | Valtion atk-varakeskus | 47 |
| | Varalaitetilat | 47 |
| | Tietoliikenteen ja verkkopalvelujen varmistaminen | 47 |
| | Varavoiman saannin varmistaminen | 48 |
| | Lähiverkot | 48 |
| | Sähköposti | 48 |
| | Toipumissuunnitelmaan siirtyminen | 49 |
| | Palaaminen normaaliin toimintaan | 49 |
| | Toipumissuunnitelman testaus | 50 |
| | Seuranta | 50 |
| | Tiedottaminen | 50 |
| | Toipumissuunnitelman säilytys | 50 |
| 7. | POIKKEUSOLOJEN VALMIUSSUUNNITELMA | 52 |
| 7.1 | Poikkeusolojen valmiussuunnittelun perusteet | 52 |
| 7.2 | Lähtökohdat | 53 |
| 7.3 | Poikkeusolojen vaikutusten arviointi | 54 |
| 7.4 | Kriittiset järjestelmät | 55 |
| 7.5 | Laitteet, varaosat, tarvikkeet ja huolto | 55 |
| 7.6 | Tietoliikenne | 56 |
| 7.7 | Logistiikka ja kuljetukset | 57 |
| 7.8 | Henkilöstö | 57 |
| | Vastuujärjestelyt | 57 |
| | Henkilövaraukset | 58 |
| | Koulutus | 58 |
| 7.9 | Ohjelmistot ja käyttö | 58 |
| 7.10 | Fyysinen turvallisuus | 59 |
| 7.11 | Energian saanti | 59 |
| 7.12 | Toimintavaihtoehdot | 60 |
| | Valmiuden kohottaminen | 60 |
| | Tietotekniikan käyttöasteen alentaminen | 60 |
| | Tietotekniikasta luopuminen | 61 |
| 7.13 | Evakuointi ja siirtyminen | 61 |
| 7.14 | Elpyminen | 62 |
| 7.15 | Testit ja valvonta | 62 |
| 7.16 | Yhteistoiminta | 62 |
| 8. | TURVALLISUUS- JA VALMIUSSUUNNITTELUN TOTEUTUS | 64 |
| 8.1 | Käynnistysvastuu | 64 |
| 8.2 | Projektin organisointi | 64 |
| 8.3 | Henkilöstön koulutus | 65 |
| 8.4 | Valvonta | 65 |
| 9. | YHDISTELMÄ | 67 |

LIITTEET

- Liite 1 Viitteet
- Liite 2 Käsitteitä
- Liite 3 Ohjeita
- Liite 4a Tietoturvallisuusvastuut ja tehtäväjako
- Liite 4b Tietojenkäsittelyn uhkatekijöitä
- Liite 4c Haavoittuvuuden ja valmiuden arviointi
- Liite 5 Tietoturvallisuuden suunnittelu

TIETOTEKNIIKAN TURVALLISUUS JA TOIMINNAN VARMISTAMINEN

ESIPUHE

Tietotekniikka on nykyään ehdottoman tärkeää yritysten, virastojen, laitosten ja koko yhteiskunnan toimivuudelle. Niin yritysten kuin julkisyhteisöjenkin palvelut, toiminta ja tuotanto ovat tietotekniikkaan sidottuja ja sen toiminnasta riippuvia. Tietotekninen kehitys on johtanut koko yhteiskunnan verkottumiseen ja verkkoriippuvuuteen. Tämä lisää tiedon ja tietotekniikan turvallisuudelle asetettavia vaatimuksia.

Yritysten operatiivisen ja tietohallinnon johdon on nähtävä tietotekniikka laadun, jatkuvuuden ja koko toiminnan kriittisenä voimavarana. Sen kehittäminen edellyttää myös tietoturvallisuuden liittämistä toimintastrategioihin ja riskienhallintaan.

Tämän suunnitteluohjeen tarkoituksena on kiinnittää yritysten ja laitosten johdon sekä toimintayksiköistä, hallinnosta ja tietojärjestelmistä vastuussa olevien esimiesten huomio verkottumisen synnyttämiin uhkiin ja tietotekniikan haavoittuvuuden seurauksena toimintaan kohdistuviin riskeihin sekä niihin toimenpiteisiin, joita tarvitaan tietoturvallisuuden suunnitelmallisessa kehittämisessä normaaliolojen, erityistilanteiden ja poikkeusolojen varalle.

Ohje on laadittu projektityönä puolustustaloudellisen suunnittelukunnan (PTS) tietojärjestelmäjaoston toimeksiannosta. Johtoryhmän puheenjohtajana on ollut apulaisjohtaja Ilkka Kananen Huoltovarmuuskeskuksesta ja jäsenenä johtaja Tarmo Eskola UPM-Kymmene Oyj:stä, turvallisuusjohtaja Erkki Heliö TietoEnator Oyj:stä, johdon konsultti Aarno Kansikas ICL Invia Oyj:stä, neuvotteleva virkamies Kaarlo Korvola sisäasiainministeriöstä ja ylitarkastaja Terttu Mellin valtiovarainministeriöstä.

Ohjeen sisällön on konsulttitoimeksiannota tuottanut toimitusjohtaja Pentti Harmanen Turvallisuustieto Oy:stä.

Tausta-aineistona on käytetty valtionhallinnolle ja yrityksille annettuja tietoturvallisuutta ja valmiussuunnittelua koskevia ohjeita ja suosituksia.

Tämä ohje korvaa PTS:n tietojärjestelmäjaoston julkaiseman ohjeen Tietojenkäsittelyn turvaaminen tietoyhteiskunnassa (1/1996). Ohjetta käytetään tietotekniikka-alan varautumisen suunnitteluperusteena.

TIIVISTELMÄ

Tavoitteena toiminnan jatkuvuuden varmistaminen

Tietoturvallisuuden tarkoituksena on koko organisaation toiminnan jatkuvuuden varmistaminen. Tiedon ja toimintaprosessien arvo on suuri. Siksi tiedon ja tietovarastojen eheyden, luottamuksellisuuden ja käytettävyyden turvaaminen on yhä tärkeämpää. Useimpien suomalaisten organisaatioiden toiminta rakentuu niin perusteellisesti tietotekniikan varaan, ettei siitä voida selviytyä ilman tietotekniikkaa eikä toisaalta sitä turvaavia, ennalta luotuja ja toteutettuja tietoturvallisuusmenettelyjä. Tietoturvallisuuden suunnittelu tähtää normaaliolojen tietoturvallisuuteen, vakavien tietoteknisten keskeytysten ja erityistilanteiden hallintaan sekä poikkeusolojen valmiuteen.

Verkkoriippuvuus on hallittava

Toiminnan riippuvuus tietotekniikasta ja monista koti- ja ulkomaisista verkko- ja tietojenkäsittelypalveluista on aikaansaanut haavoittuvan tuotantoympäristön. Toimintaa uhkaavat tekijät ovat moninaisia. Laajoissa verkottuneissa tietojärjestelmissä itse järjestelmän ja järjestelmähallinnan hajautuminen johtaa turvallisuuden vaikeaan hallintaan. Erityisen ongelmallisia ovat pääsyn- ja käytönvalvonta, prosessien toiminnan ja eheyden ylläpito, tietoliikenteen suojaaminen, tietovarastojen varmistaminen sekä käyttöympäristön valvonta. Turvallisuuden puutteet voivat johtaa tietojen menetyksiin ja kokonaisten tietojärjestelmien keskeytyksiin ja siten vakaviin vahinkoihin varsinaisessa toiminnassa.

Ulkoistaminen ja tietoturvallisuus

Tietotekniikan korkeat osaamisvaatimukset, teknisen kehityksen nopeus ja siitä seuraavat taloudellisuus- ja tehokkuusvaatimukset ovat keskittäneet tietotekniikkapalvelut palveluyrityksiin. Verkottuminen puolestaan on johtanut riippuvuuteen verkko-operaattoreista, ei ainoastaan kotimaisista vaan myös kansainvälisistä operaattoreista. Ulkoistamisen ja verkottumisen seurauksena turvallisuuden hallinta edellyttää turvallisuustoimenpiteitä myös näiltä toisilta osapuolilta. Tietoturvallisuuden tasosta tinkimättä on tehtävät jaettava eri osapuolten välillä sopimuksin. Tietoturvallisuus on siten myös yhteistoimintaa, jossa eri osapuolten on kannettava vastuunsa palvelujensa turvallisuudesta ja varmistamisesta. On kuitenkin muistettava, että vastuu on lopulta aina palveluja käyttävällä organisaatiolla.

Tietosodankäynti ja uudet uhat

Maailmanlaajuinen verkottuminen mahdollistaa aivan uudenlaiset tietojärjestelmiin kohdistuvat hyökkäykset. Niiden tarkoituksena saattaa olla tahallinen häirintä, teollisuusvakoilu, toiminnan estäminen, tietojen tuhoaminen tai virus- ja haittaohjelmien levittäminen. Tekijöinä eivät ole yksinomaan harrastelijat vaan yhä useammin omat työntekijät, kilpailevat yritykset, järjestäytyneet rikolliset, ääriliikkeet, terroristiryhmät sekä valtiolliset tiedusteluorganisaatiot. Hyökkäykset voivat kuulua tietosodankäyntiin, jota käydään jatkuvasti mm. tietojärjestelmiin tunkeutumalla.

Uhanalaisia näille tietoriskeille ovat tärkeillä aloilla toimivat valtionhallinnon organisaatiot, korkean teknologian yritykset, tietoliikenne- ja viestintäorganisaatiot, rahoituslaitokset sekä muut tärkeät yritykset ja yhteisöt.

Muutosvalmiutta tarvitaan

Toimintaympäristö muuttuu nopeasti. Teknisten muutosten ohella huomattavia ovat yritysrakenteiden muutokset, jotka johtuvat tietotekniikka-alan, teletoinnin ja tiedonsiirtopalvelujen keskittymisestä sekä muista yhteiskunnallisista ja kansainvälisistä tekijöistä vaikeuttaen tietoturvallisuuden järjestelyä ja hallintaa.

Varautuminen

Varautuminen vakaviin tietojärjestelmien, -yhteyksien ja -palvelujen keskeytyksiin on tullut entistä tärkeämmäksi. Keskeytysten vaikutukset ulottuvat käyttäjäorganisaation ohella myös laajaan asiakaskuntaan ja yhteistyötahoihin. Keskeytys laajan järjestelmäkokonaisuuden osassa tai yhteyksissä saattaa rajoittaa tietojenkäsittelyä tai jopa estää sen kokonaan. Erittäin pahoin toimintaa uhkaavia ovat keskeytykset pitkissä logistiikka- ja palveluketjuissa.

Eriytilanteet

Teknisten järjestelmien ja erityisesti perusrakenteiden ja verkkojen keskeytykset voivat pahimmillaan johtaa kaikkia organisaatioita koskeviin erityistilanteisiin. Tällöin ongelmat muistuttavat poikkeusolojen tietotekniikan vaikeuksia. Toiminnan ja tietotekniikan kannalta tämä edellyttää varautumista pahimpiin tietotekniikan uhkakuviin.

Poikkeusolojen tietojenkäsittely

Poikkeusoloilla tarkoitetaan alueellisesti tai valtakunnallisesti vaikeutuneita toimintaolosuhteita, jolloin valmiuslain mukaiset viranomaisten ohjaus- ja säännöstelyvaltuudet voidaan ottaa käyttöön. Poikkeusolot edellyttävät ennalta luotujen valmiussuunnitelmien toimeenpanoa yritysten ja julkisyhteisöjen toiminnan jatkamiseksi ja kansallisten ehtojen turvaamiseksi.

Poikkeusoloissa tietojenkäsittelyyn vaikuttavat omien ja ulkopuolisten resurssien vähentyminen, muuttunut tietotekninen ympäristö sekä laajavaikeutiset tiedonsiirtoyhteyksien, varaosien ja ohjelmistotuen puutteet, vahingot, vakoilu, tietojärjestelmien sabotointi ja tietosodankäynti sekä vakavat fyysiset vauriot. Poikkeusolojen toiminnalle tietotekniikkariippuvuus ja erityisesti verkkoriippuvuus ovat kriittisiä tekijöitä. Päätettäessä tärkeiden organisaatioiden toimintastrategioista, tietohallinnosta ja tietotekniikan kehittämisestä onkin tärkeää huomioida poikkeusolojen toiminnan varmistamistarpeet. Hyvin toimivien logistiikkaketjujen varassa voidaan toimia normaalioloissa. Poikkeusoloissa toimintaedellytykset menetetään helposti, ellei varautumistoimenpiteitä ole suunniteltu.

Strateginen merkitys

Yhä useampien yritysten strategiat rakentuvat tietotekniikan varaan. Siksi strategisessa suunnittelussa on tietoteknisten vahvuuksien ohella otettava huomioon myös ne uhat ja heikkoudet, jotka johtuvat puutteellisesta tie-

toturvallisuudesta ja jotka voivat vaarantaa strategisen toiminnan jatkuvuuden. Tietoturvallisuutta on rakennettava palvelukykyvaatimusten mukaisesti. Tietoturvallisuus parantaa selkeästi toiminnan laatua ja kuuluu hyvään tiedonhallintatapaan. Sen tulee vastata sidosryhmien vaatimuksia sekä organisaation toiminnan tasoa.

Kehittäminen

Turvallisuuden saattamiseksi toiminnan ja tietojenkäsittelyn vaatimalle tasolle organisaation ylimmän johdon on päätettävä turvallisuuden kehittämisestä ja sitouduttava kehitystyöhön sekä tarjottava sen vaatimat resurssit.

Organisaation toiminnan laadusta ja nykyisistä toimenpiteistä riippuen kehittämistyöhön kuuluu turvallisuuspolitiikka sekä perusturvallisuuden ja poikkeusolojen valmiuden linjaukset. Lähtökohtana tulee olla uhkien ja riskien tunnistaminen ja niiden arviointi. Suunnittelun tärkeimpiä tehtäväkokonaisuuksia ovat tavoitteiden asettaminen, koko organisaation vastuujärjestelyt, kehittämiskohteiden ja -tarpeiden määrittely, tietojärjestelmien ja järjestelmänosien priorisointi sekä tietoturvallisuuden suunnittelu normaaliolojen ja poikkeusolojen varalle.

Tietoturvallisuusvastuut

Organisaatioiden kaikkien toimintojen riippuvuus tietotekniikasta on muuttanut turvallisuuden vastuusuhteita. Turvallisuuden lähtökohtana ovat varsinaisen toiminnan - tuotannon, palvelujen ja hallinnon - tarpeet. Ne tuntien tulee nähdä toiminnalle välttämättömät tiedot, tietovarastot, tietojärjestelmät ja tietoverkot. Turvallisuuden kehittäminen ja ylläpito on mahdollista vain silloin, kun toiminnasta vastuussa oleva johto ja tietojärjestelmien omistajat tuntevat riskit ja riippuvuudet ja kykenevät vastualueellaan huolehtimaan tietoturvallisuudesta omistajien, asiakkaiden, henkilökunnan, muiden sidosryhmien, yhteiskunnan ja yhteistyökumppanien odotusten mukaisesti. Johdon päätökset ja toimenpiteet vastuun ohjaamiseksi ovat tässä tärkeitä.

Suunnitelmat

Varmistaminen vaatii ennalta toteutettua tietoteknistä ja fyysistä turvallisuutta sekä valmiutta toimia häiriötilanteissa ja toipua niistä. Valmiuden luomiseen tarvitaan kokonaisvaltaiseen suunnitelmaan perustuvia toimenpiteitä vahinkojen välttämiseksi normaalioloissa, menetysten rajoittamiseksi vakavissa keskeytyksissä sekä toiminnan ylläpitämiseksi poikkeusoloissa.

Perusturvallisuuden tietoturvallisuus- ja toipumissuunnitelmat ovat välttämättömiä kaikissa tietotekniikasta riippuvissa organisaatioissa. Puolustaloudellisessa varautumisessa tärkeysluokiteltujen yritysten on tarpeen laatia lisäksi poikkeusolojen tuotantoa tukeva tietojenkäsittelyn valmiussuunnitelma.

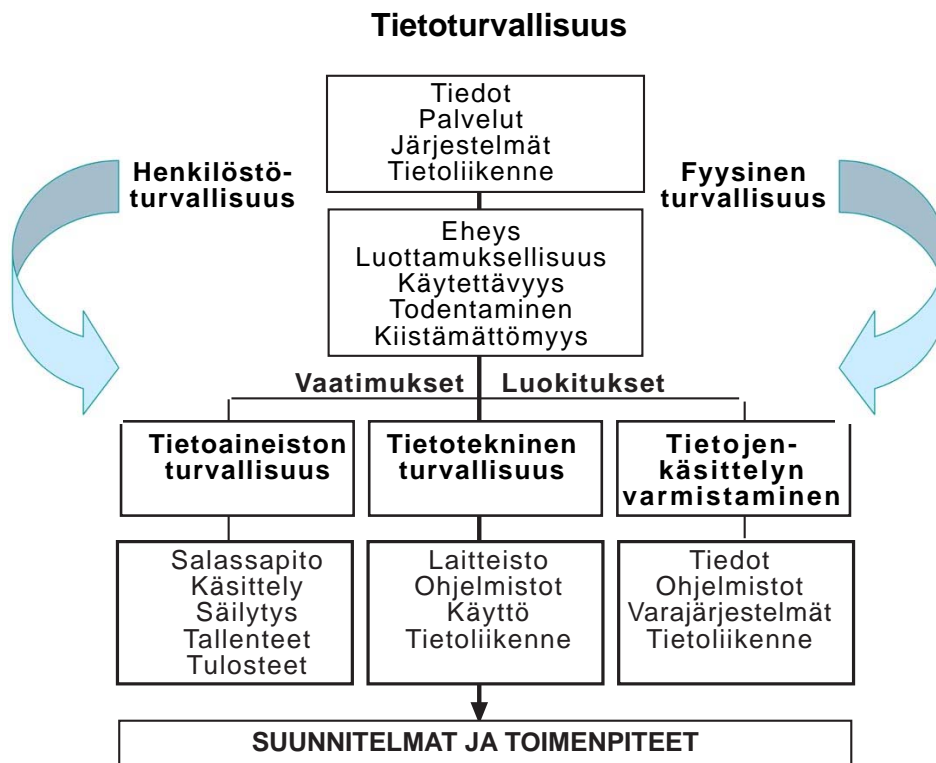
Yhteiskunnallinen vastuu

Yhteiskunnan toimivuuden turvaaminen edellyttää yritysten tärkeiden toimintojen varmistamista ja tietojenkäsittelyn turvaamista kaikissa olosuhteissa. Yritysten yhteiskunnallinen vastuu korostuu poikkeusoloissa.

1. JOHDANTO

Monilla aloilla suomalaisilla yrityksillä on kansainvälistä huipputasoa. Myös tietotekniikan käytössä suomalaiset yritykset ja laitokset ovat kansainvälisesti korkealla tasolla. Monien organisaatioiden toiminta riippuu täysin tietojärjestelmien, tiedonsiirron, verkkopalvelujen ja sähköpostin toimivuudesta. Ilman tietoturvaluottuutta ja siihen sisältyvää tietotekniikan varmistamista alttius tietojen menetyksiin, luvattomuuksiin ja palvelujen kriittisiin keskeytyksiin on erittäin suuri. Tietoturvaluottuuden puutteista johtuvat vahingot saattavat aiheuttaa organisaation toiminnalle vakavia, jopa ylitsepääsemättömiä vaikeuksia.

Tietoturvaluottuudella tarkoitetaan organisaation toiminnan turvaamista suojaamalla tietoaaineisto ja tietotekniikka, vähentämällä virheiden, väärinkäytösten, häiriöiden ja fyysisten vahinkojen riskiä, varautumalla niihin ennalta ja toteuttamalla toiminnan jatkuvuuden turvaavat tietotekniikkajärjestelyt.



Tietoturvaluottuuden olennaisin tehtävä on itse tiedon suojaaminen. Tietoyhteiskunnassa tieto on arvokasta ja muodostaa ainutkertaisia tietovarastoja. Tietojen eheyden, luottamuksellisuuden ja käytettävyuden varmistaminen, käyttäjän todentaminen ja tapahtumien kiistämättömyys ovat tietojenkäsittelyn perusedellytyksiä.

Suuren tietotekniikkariippuvuuden ja siitä johtuvien laajavaikutteisten riskien seurauksena on raja tietojenkäsittelyn normaaliolojen ja poikkeusolojen varmistamistarpeiden välillä häviämässä. Laajojen järjestelmäkokonaisuuksien ylläpito, verkot sekä kansalliset ja kansainväliset verkko-

palvelut edellyttävät jo normaalioloissa varautumista häiriöihin ja laajavai-
kutteisiin keskeytyksiin, joiden ennen ajateltiin kuuluvan vain poikkeusolo-
loihin. Erityisen uhanalaisia ovat laajat logistiikka- ja palveluketjut. Tä-
män vuoksi perusturvallisuudessa tulee tavanomaisten tietoriskien ohella
varautua myös näihin tietoteknisiin erityistilanteisiin.

Ei riitä, että tietojenkäsittelyn varmistaminen aloitetaan vasta häiriön sat-
tuessa. Jatkuvuuden varmistaminen edellyttää ennalta toteutettuja tie-
toturvallisuuden ja fyysisen turvallisuuden toimenpiteitä sekä perusteellista
suunnittelua ja harjoittelua valmiuden luomiseksi häiriötilanteista toipumi-
seksi.

Tietotekniikan poikkeusolojen valmiusvaatimuksia voidaan tarkastella kah-
desta näkökulmasta. Toisaalta vaatimuksien asettajana ovat organisaation
oman toiminnan palvelutaso- ja jatkuvuustarpeet, toisaalta yhteiskunnan
asettamat valmiusvaatimukset hallinnon ja elinkeinoelämän turvaamiseksi
poikkeusoloissa. Tietojenkäsittelyn poikkeusolojen valmiudessa on kiin-
nitettävä huomiota erityisesti kansainvälisten verkkojen yli hoidettavien
palvelujen keskeytymiseen. Poikkeusolot etäälläkin voivat aikaansaada
erityisolosuhteita, joissa tietojenkäsittely verkoissa keskeytyy.

Maailmanlaajuinen palveluverkko



Poikkeusoloissa toimintaan vaikuttavat mm. tietotekniikan varaosien saan-
nin tyrehtyminen, kauppapoliittiset rajoitukset, kansainvälisten tietoliiken-
neyhteyksien katkeaminen ja vakavat ulkoiset kriisit.

Keskeistä tietojenkäsittelyn turvaamisessa ja varmistamisessa on:

- uhkien arviointi
- riskien ja haavoittuvuuden selvittäminen
- tietoturvallisuuden perustason luominen siten, että se edistää toiminnan varmistamista myös poikkeusoloissa
- valmiuksien kehittäminen yleisimpien ongelmatilanteiden ja erityistilan-
teiden varalle
- suunnitelmien laatiminen vakavien häiriöiden hallitsemiseksi
- valmiuden luominen poikkeusolojen toiminnalle.

Tämän ohjeen tavoitteena on normaaliajan perusturvallisuuden ja poikkeusolojen valmiussuunnittelun muodostaman kokonaisuuden ja tavoitteiden kuvaaminen sekä valmistelun tukeminen ja edistäminen.

Ohjeen toisessa luvussa kuvataan tietoturvallisuuteen ja toiminnan jatkuvuuteen vaikuttavat tekijät ja turvallisuuden vaatimukset normaali- ja poikkeusoloissa. Kolmas luku lähestyy valmiussuunnittelua organisaation toiminnan, johtamisen ja vastuunjaon näkökulmasta. Neljännessä luvussa tarkastellaan tietojenkäsittelyyn normaali- ja poikkeusoloissa kohdistuvia uhkia ja niiden arviointia toiminnan ja tietojenkäsittelyn suunnasta. Viidennessä luvussa käsitellään turvallisuuden ja varautumisen tavoitteita ja vaatimuksia. Kuudennessa, seitsemännessä ja kahdeksannessa luvussa kuvataan perusturvallisuuden ja poikkeusolojen valmiuden sisältö ja suunnittelun pääkohdat. Yhdeksännessä luvussa esitetään suuntaviivat valmiussuunnitteluprojektin järjestelylle, toteutukselle ja valvonnalle. Yhdistelmään on koottu pääasialliset johdon toimenpiteet valmiussuunnittelun kehittämiseksi.

Tekstin viitenumerot viittaavat lähdeaineistoon liitteessä 1. Käsitteitä on esitetty liitteessä 2. Luettelo ajankohtaisista ohjeista on liitteenä 3. Tietoturvallisuudesta vastaavien henkilöiden tehtävät on esitetty liitteessä 4a. Tietoturvallisuuden uhkien ja riskien arviointi on esitetty liitteessä 4b. Liitteessä 4c on esitetty tietoturvallisuuden kartoituksessa ja suunnittelussa käsiteltäviä seikkoja. Liitteeseen 5 on koottu yksityiskohtaiset esimerkit suunnitelmissa käsiteltävistä asioista.

2. TOIMINNAN TURVALLISUUTEEN JA JATKUVUUTEEN VAIKUTTAVAT TEKIJÄT

2.1 Lähtökohdat

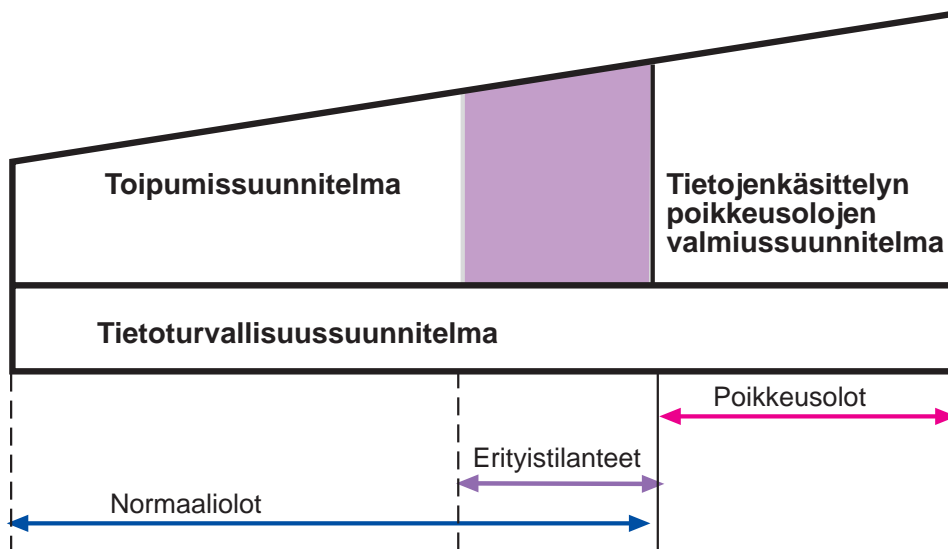
Tietoriskien hallinnan tulee perustua toimintojen ja palvelujen tietotekniikkariippuvuuksien ja tiedon turvaamistarpeiden tuntemiseen sekä sen perusteella tehtyihin ratkaisuihin. Tietoturvallisuus ei voi perustua vain tietotekniisiin lähtökohtiin.

Turvallisuus- ja valmiussuunnittelun päätavoitteita ovat:

- normaalioloihin liittyvien uhkien ja riskien hallinta
- varautuminen keskeytyksiin ja tietoteknisten erityistilanteiden hallintaan vahinkojen välttämiseksi ja rajoittamiseksi
- valmiuden luominen toiminnalle poikkeusoloissa.

Suunnittelu käsittää perusturvallisuuden - tietoturvaluussuunnittelun ja toipumissuunnittelun - sekä tietojenkäsittelyn poikkeusolojen valmiussuunnittelun. Kokonaisuudessaan on kysymys organisaation toiminnan jatkuvuuden varmistamisesta eri olosuhteissa turvaamalla sen tiedot ja tietojenkäsittely. Itse tuotantotoiminnan valmiussuunnittelusta puolustustaloudellinen suunnittelukunta on antanut ohjeet erikseen.

Toiminnan jatkuvuuden varmistaminen



Jo normaalioloissa voi syntyä erityistilanteita, joissa tietotekniikan käytön varmistamiseen on varauduttava joiltakin osin samoin kuin poikkeusoloissa.

2.2 Tietoturvallisuuden yleiset tavoitteet

Tietojenkäsittelyn turvallisuuden perustavoitteina on tiedon eheyden, luottamuksellisuuden ja käytettävyyden varmistaminen sekä todentaminen ja kiistämättömyys.

Eheys käsittää tietoaineistojen ja tietojärjestelmien suojaamisen siten, etteivät tiedot laitteisto- ja ohjelmistovikojen, tuhojen tai oikeudettoman toiminnan takia muutu tai tuhoutu. Erityisesti laajoissa tietojärjestelmissä, joissa tiedonhallinta ja tietovarastot on hajautettu verkon osiin, eheyden säilyttäminen vaatii erityistä huomiota ja järjestelmähallinnan toimenpiteitä.

Luottamuksellisuus käsittää tiedon suojaamisen ja valvonnan siten, että tiedot ovat vain niiden käyttöön oikeutettujen henkilöiden saatavilla eikä niitä paljasteta tai saateta sivullisten käyttöön. Luottamuksellisuuden soveltaminen käytäntöön tapahtuu tietojen luokituksella ja siitä seuraavalla salassapidolla sekä luokituksen perusteella tietojenkäsittelyyn luoduilla suojausmenettelyillä.

Käytettävyydellä tarkoitetaan, että tietojärjestelmien tiedot ja palvelut ovat tarvittaessa esteettä niiden käyttöön oikeutettujen saatavilla.

Todentaminen tarkoittaa järjestelmän käyttäjän (henkilön, organisaation tai laitteen) tai viestinnässä toisen osapuolen tunnistuksen varmistamista. Se tapahtuu käyttäjätunnuksella ja salasanalla (yksinkertainen tunnistus), salausmenetelmin (vahva tunnistus) tai varmentein (sähköinen toimikortti).

Kiistämättömyys tarkoittaa tapahtuneen todistamista jälkeensä, jolloin tavoitteena on juridinen sitovuus. Kiistämättömyys varmistaa, ettei toinen osapuoli voi kieltää toimintaansa jälkeensä (alkuperän, luovutuksen, vastaanoton ja tapahtuman kiistämättömyys). Kiistämättömyys aikaansaadetaan sähköisin allekirjoituksin.

Eheys-, luottamuksellisuus-, käytettävyys-, todennus- ja kiistämättömyysvaatimukset koskevat tietojenkäsittelyä kaikissa oloissa.

2.3 Tietoturvallisuuden tavoitteet toiminnan näkökulmasta

Tietoturvallisuuden tavoitteita organisaation näkökulmasta ovat:

- organisaation tietojen ja osaamisen säilyttäminen kilpailukyvyn varmistamiseksi
- tietoon ja tietotekniikkaan perustuvien palvelujen ja toimintojen turvaaminen sekä tietotekniikkariippuvuuden hallitseminen
- tietojenkäsittelyn virheettömyyden varmistaminen ja tietojenkäsittelystä riippuvan laadun ylläpitäminen
- tietojenkäsittelyn tehokkuuden ylläpitäminen ja tuotannon keskeyttämättömyyden varmistaminen
- valmius toiminnan jatkamiseen keskeytystenkin sattuessa
- hyvä tiedonhallintatapa
- luotettavuuden ja yrityskuvan säilyttäminen.

Käytännössä turvallisuus toteutetaan toimenpiteillä, jotka kohdistuvat

- hallinnolliseen tietoturvaluuteen
- henkilöstöturvallisuuteen
- tietoaineiston turvallisuuteen
- tietotekniseen turvallisuuteen
 - laitteistoturvallisuuteen
 - ohjelmistoturvallisuuteen
 - tietoliikenneturvallisuuteen
 - käyttöturvallisuuteen
- fyysiseen turvallisuuteen.

Tietotekniikka on syrjäyttänyt manuaaliset järjestelmät siten, ettei toiminnissa tarvittavia prosesseja voida enää hoitaa ilman tietotekniikkaa. Siksi tietotekniikan käytön edellytykset on poikkeusoloissakin turvattava olosuhteiden sallimalla, ennalta valmistellulla tasolla.

2.4 Normaaliolojen tietojenkäsittelyn varmistaminen

Verkkoriippuvuuden, palvelujen ulkoistamisen sekä koti- ja ulkomaisen palveluriippuvuuden vuoksi tietojenkäsittely on jo normaalioloissa haavoittuva. Luotettava tietojenkäsittely edellyttää perusturvallisuutta joka-päiväisessä toiminnassa esiintyviin turvallisuusriskien hallintaan.

Keskeytyksiin johtavia vahinkoja voi sattua monissa järjestelmän osissa teknisten häiriöiden, tietoliikennevikojen tai tietoverkoista tapahtuvan tahallisen häirinnän seurauksena tai erityistilanteista johtuen. Organisaatioissa on oltava valmius varajärjestelmien käynnistämiseen toiminnalle koituvien vahinkojen rajoittamiseksi ja toiminnan palauttamiseksi normaaliksi.

Valtioneuvoston asettama tietoturvaluusasioiden neuvottelukunta toimii kansalaisten, yritysten, järjestöjen ja viranomaisten välisenä yhteistyöelimenä normaalioloihin liittyvissä tietoturvaluuskysymyksissä. Sen tehtävänä on seurata tietoturvaluuden tilaa ja hankkeita, antaa ehdotuksia toimenpiteistä, lisätä kansalaisten, yritysten ja viranomaisten yhteistyötä tietoliikenteen ja tietojärjestelmien turvallisuuteen liittyvissä asioissa sekä tehdä ehdotuksia kansalliseksi tietoturvalustrategiaksi ja edistää tietoturvaluuteen liittyvää teknologiaa ja osaamista.

2.5 Poikkeusolojen toiminta ja tietojenkäsittelyn varmistaminen

Poikkeusoloissakin toiminta rakentuu tietotekniikan varaan. Tietotekniikkariippuvuuden hallinta on poikkeusolojen valmiudelle ratkaisevaa ja edellyttää välttämättä turvallisuus- ja varmistamistarpeiden huomioon ottamista päätettäessä strategioista, tietohallinnosta, tietotekniikan kehittämisestä ja hankinnoista.

Poikkeusoloissa haavoittuvuuteen vaikuttavat omien ja ulkopuolisten resurssien väheneminen, muuttunut toimintaympäristö sekä laajavaikuttaiset tiedonsiirtoyhteyksien, varaosien ja ohjelmistotuen puutteet, vahingot, vakoilu, tietojärjestelmien sabotointi, tietosodankäynti ja vakavat fyysiset vauriot.

Kriisitilanteessa ei enää ole mahdollisuuksia eikä aikaa luoda poikkeusolojen valmiutta. Oman, asiakkaiden ja yhteiskunnan toiminnan turvaamiseksi valmiuksien on oltava ennalta luotuja. Kriisinkestokykyä parantavat olennaisesti hyvin toteutettu perusturvallisuus ja varajärjestelmin aikaansaatu toipumisvalmius. Tärkeillä elinkeinoelämän alueilla valmiuden puuttuminen johtaa yhteiskunnan toimintojen haavoittumiseen.

2.6 Puolustustaloudellinen varautuminen

Poikkeusolot

Poikkeusoloja, jolloin valmiuslain¹ mukaiset ohjaus- ja säännöstelyvaltuudet voidaan ottaa käyttöön ovat:

- Suomeen kohdistuva aseellinen hyökkäys ja sota sekä sodan jälkitila,
- Suomen alueellisen koskemattomuuden vakava loukkaus ja maahan kohdistuva sodanuhka,
- vieraiden valtioiden välinen sota tai sodanuhka ja sellainen sodanuhkaa merkitsevä vakava kansainvälinen jännitystila, joka edellyttää välttämättömiä toimenpiteitä Suomen puolustusvalmiuden kohottamiseksi, sekä muu vaikutuksiltaan näihin verrattava Suomen ulkopuolella sattunut erityinen tapahtuma, jos siitä voi aiheutua vakava vaara laissa tarkoitettulle kansallisen olemassaolon ja hyvinvoinnin perusteille, edellyttäen, että tilanteen hallitseminen ei ole mahdollista viranomaisten säännönmukaisin toimivaltuuksin,
- välttämättömien polttoaineiden ja muun energian sekä raaka-aineiden ja muiden tavaroiden tuonnin vaikeutumisesta tai estymisestä taikka muusta vaikutuksiltaan näihin verrattavista kansainvälisen vaihdannan äkillisestä häiriintymisestä aiheutuva vakava uhka väestön toimeentulolle tai maan talouselämän perusteille,
- suuronnettomuus edellyttäen, että tilanteen hallitseminen ei ole mahdollista viranomaisten säännönmukaisin toimivaltuuksin.

Nämä poikkeusolot ovat valmiussuunnitelmien ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmistelujen kehyksinä.

Huoltovarmuus ja sen yleistavoitteet

Huoltovarmuudella tarkoitetaan väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömien taloudellisten toimintojen turvaamista poikkeusolojen varalta.²

Valtioneuvoston päätöksen mukaan taloudellisen varautumisen yleistavoitteena on turvata kansallisiin toimenpiteisiin ja voimavaroihin perustuva huoltovarmuus. Tavoitteena on, että yhteiskunta selviytyy 12 kuukautta kestävästä kriisistä, jolloin ulkomaankauppa on osittain estynyt.³ Tällöin yhteiskunnan ja talouselämän toiminnot on mitoitettu perushuollon edellyttämälle tasolle, jonka kukin ministeriö määrittelee omalla hallinnonalallaan. Perushuoltotasolle siirrytään asteittain kansainvälisen tilanteen kiristyessä.

Huoltovarmuuden turvaamiseksi kaikissa oloissa on luotava ja ylläpidettävä riittävä valmius hyödykkeiden tuottamiseksi sekä tuotannon, jakelun, kulutuksen ja ulkomaankaupan ohjaamiseksi.³

Huoltovarmuuden painopistealueet ovat:

- yhteiskunnan tekniset perusrakenteet
- kuljetus-, varastointi- ja jakelujärjestelmät
- elintarvikehuolto
- energiahuolto
- sosiaali- ja terveydenhuolto
- sotilaallista maanpuolustusta tukeva teollisuustuotanto ja järjestelmien ylläpito.

Yhteiskunnan toimivuuden turvaaminen on noussut huoltovarmuuden keskeiseksi painopisteeksi, mikä merkitsee panostamista kriittisten teknisten, erityisesti tietoteknisten järjestelmien varmistamiseen.

Varautumisessa keskitytään yhteiskunnan toimivuuden kannalta kaikkein kriittisimpien perusjärjestelmien varmistamiseen. Lisäksi näiden ylläpitämiselle välttämättömän elektroniikka- ja sähköteknisen teollisuuden toimintaedellytykset turvataan. Turvattavia teknisiä perusrakenteita ovat energiaverkot, tietoliikenneverkot, keskeiset tietojärjestelmät, sähköinen ja painettu joukkoviestintä, rahoitustoiminta, maksuliike, rahahuolto, tietoteknologian huolto- ja ylläpitopalvelut, vesihuolto ja muut keskeiset kunnallistekniset peruspalvelut. Myös kuljetukset ja niihin liittyvät logistiset järjestelmät muodostavat yhteiskunnan toimivuuden kannalta välttämättömän kokonaisuuden.³

Teleyrityksen tulee varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa osallistumalla teletoiminnan valmiussuunnitteluun ja valmistelemalla etukäteen poikkeusoloissa tapahtuvaa toimintaa sekä muin toimenpitein.⁴

Valmiuslainsäädännön tarkoittamien poikkeusolojen lisäksi pyritään varautumaan myös muihin huoltovarmuutta uhkaaviin kriiseihin ja vakaviin markkinahäiriöihin sekä entistä enemmän normaaliolojen häiriöihin.

Puolustustaloudellinen suunnittelu

Normaaliolojen hallinto ja talouselämä muodostavat sen perustan, jolta toimintavalmiutta kehitetään myös poikkeusoloihin. Huoltovarmuuden turvaamisessa keskeisintä on kansalaisia palvelevien ja taloutta tukevien perustoimintojen jatkuvuuden turvaaminen (organisatorinen huoltovarmuus) sekä tuotannon kannalta kriittisten tavaroiden saatavuuden turvaaminen (materiaalinen huoltovarmuus).

Taloudellista puolustusvalmiutta ja talouselämän turvaamista poikkeusoloissa koskevat suunnittelu-, selvitys- ja järjestelytehtävät kuuluvat kauppa- ja teollisuusministeriön alaiselle puolustustaloudelliselle suunnittelukunnalle (PTS) ja Huoltovarmuuskeskukselle (HVK).

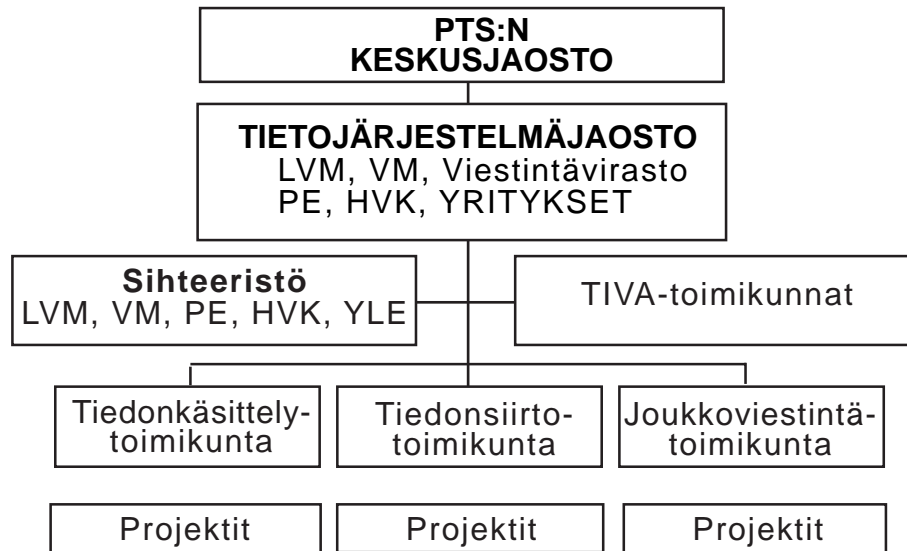
Suunnittelunsa perusteiksi PTS voi velvoittaa organisaatioita antamaan sen tarvitsemia tietoja tuotannosta, laitteista, niiden käytöstä, henkilöstöstä ja muista seikoista.^{5, 6}

Tietojärjestelmäalan varautuminen

PTS:n tietojärjestelmäjaoston päätavoitteena on tiedonkäsittelyn ja -siirron sekä joukkoviestinnän kehityspiirteiden seuranta ja analysointi sekä huol-

tovarmuuden yhteensovittaminen ja edistäminen. Jaostolla on tietojenkäsittelytoimikunta, tiedonsiirtotoimikunta ja joukkoviestintätoimikunta sekä sihteeristö. Koko tietojärjestelmälän valmiussuunnittelu on näin koottu yhdeksi kokonaisuudeksi. Jaoston alueellisen organisaation muodostavat tietojärjestelmälän valmiustoimikunnat (TIVA-toimikunnat). Ne hoitavat alueelliseen varautumistoimintaan liittyviä tehtäviä lääninhallitusten yhteydessä.

Sähköisen viestinnän valtakunnallinen varautumisorganisaatio



Yritysten tärkeysluokitus

Kriisiaikaisten toimintaedellytysten luomista ja ylläpitämistä ohjataan yritysten ja viranomaisorganisaatioiden tärkeysluokituksella. PTS:n elimet ja pääesikunta luokittelevat yritykset ja toimipaikat. Tietojenkäsittelyalalla PTS:n tietojärjestelmäjaosto tekee luokittelun ja HVK vahvistaa sen vuosittain. Valtionhallinnossa vastaavan luokittelun tekee valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI).

Valtakunnallisesti tärkeysluokiteltuja yrityksiä ovat ensi sijassa

- perushuollon turvaamiseen tarvittavat valtakunnallisesti korvaamattomat yritykset ja valtakunnallisesti tärkeä energiahuolto
- valtakunnan infrastruktuurin kannalta tärkeät yritykset ja laitokset
- kriisiajan ulkomaankaupan kannalta korvaamattomat, strategiset vientiyritykset
- puolustusvälinetuotannon kannalta korvaamattomassa asemassa olevat yritykset
- yritysten korvaamattomat alihankkijat ja raaka-ainetuottajat
- valtakunnallisesti elintärkeät energian jakeluun liittyvät laitokset
- valtakunnallisesti elintärkeät tuotteiden jakeluun ja kuljetukseen liittyvät liikelaitokset ja keskusvarastot
- alueellisesti väestön toimeentulon tai sotilaallisen toiminnan kannalta välttämättömät yritykset ja liikelaitokset
- paikalliseen energiantuotantoon ja jakeluun, veden- ja lämmönjakeluun sekä viestintään liittyvät laitokset.

Valtakunnalliseen luokitteluun sisällytetyt yritysten toimipaikat jaetaan kahteen tärkeysluokkaan perushuoltoon liittyvän merkityksen perusteella ottaen huomioon myös valmiussuunnittelun asteen. *Ensimmäiseen tärkeysluokkaan* kuuluu valtakunnallisesti tärkeiden yritysten toimipaikkoja. Niihin tulee nimetä valmiuspäällikkö, jonka johdolla laaditaan yrityksen valmiussuunnitelma. *Toiseen tärkeysluokkaan* kuuluu suurten yritysten toimipaikkojen lisäksi myös alihankkijoiden ja raaka-ainetoimittajien toimipaikkoja.

Valtion luokituksen piiriin kuuluu ministeriöitä, virastoja ja laitoksia sekä muita julkisen sektorin organisaatioita.

Tärkeysluokitus on perustana viranomaisten päättäessä valmiussuunnittelusta, kriisiaikaisista toimintaedellytyksistä, suojaamisesta, energiansaannin, kuljetusten, tietotekniikan varaosien, raaka-aineiden ja työvoiman saannin turvaamisesta sekä muiden voimavarojen ohjaamisesta ja säännöstelystä.

Elinkeinoelämän varautuminen ja vastuut

Yksityisellä sektorilla tietoturvallisuuden ja valmiussuunnittelun lähtökohina ovat yritysten omat normaaliolojen toiminnan turvallisuus- ja jatkuvuusvaatimukset. Yrityksen ylimmälle johdolle kuuluu vastuu edellytysten luomisesta tietoturvallisuuden toteuttamiseksi ja kehittämiseksi kokonaisuutensa osana sekä vastuu poikkeusoloihin varautumisesta.

Yrityksissä poikkeusolojen valmiutta kehitetään PTS:n antamien alakohdainten suositusten ja suunnitteluohjeiden mukaan. Suositusten taustalla ovat eri alojen yrityksiä edustavien PTS:n poolien tai toimikuntien suunnitelmat.

Elinkeinoelämän yritykset ja järjestöt saavat valmiussuunnittelunsa perusteet ja tavoitteet PTS:ltä. Keskeinen kriteeri tehtävän määrittelyssä on organisaation merkitys väestön toimeentulon, talouselämän ja taloudellisen puolustusvalmiuden (perustoimintojen) kannalta. Sotilaalliselle maanpuolustukselle tärkeät yritykset saavat valmiussuunnittelulle perusteita myös suoraan puolustusvoimilta.

Julkishallinnon varautuminen ja vastuut

Asetuksessa valtionhallinnon tietohallinnosta asetetaan tietohallinnon tavoitteeksi taloudellisuus, turvallisuus, toiminnallinen yhteensopivuus ja tietosuojan vaatimusten täyttäminen.⁷ Valtioneuvoston periaatepäätöksessä valtionhallinnon tietohallinnon kehittämisestä määrätään, että kunkin ministeriön, viraston ja laitoksen on huolehdittava siitä, että niiden tietojärjestelmien käytettävyyden ja palvelukyky ovat korkeatasoisia.⁸ Tietoturvallisuuden hallintaa ja ohjausta varten viranomaisilla tulee olla ajantasainen tiedonkäsittelyn turvaamissuunnitelma, vahinkojen varalta toipumissuunnitelma ja poikkeusolojen varalta tiedonkäsittelyn valmiussuunnitelma. Suunnitelmiin sisältyy organisaation tiedonkäsittelyriippuvuuden, tietotekniikan käyttöön liittyvien uhkatekijöiden ja riskien arviointi sekä niiden hallinnan edellyttämien turvaamis-, toipumis- ja varautumistoimenpiteiden määrittely ja toteuttamissuunnitelmat.⁹

Valtionhallinnossa

- tietoturvallisuuden yleinen ohjaus kuuluu valtiovarainministeriölle⁸
- liikenne- ja viestintäministeriö ohjaa sähköisen viestinnän tietoturvallisuusjärjestelyjä ja poikkeusoloihin varautumista
- viestintävirasto ohjaa ja valvoo tietoverkkojen tietoturvallisuutta tietoyhteiskunta-asioiden teknisenä asiantuntijaviranomaisena sekä havainnoi ja selvittää tietoturvallisuuden loukkauksia (CERT-toiminta)
- valmiussuunnittelua ja tietoturvallisuutta hallinnonalallaan ohjaa ja valvoo asianomainen ministeriö
- käytännön suunnittelutehtävistä vastaa virastokohtainen valmiuspäällikkö
- valmiussuunnittelutoimintaa koordinoivat PTS (PTS:n tietojärjestelmäjohto ja sen toimikunnat), HVK sekä puolustusministeriö ja turvallisuus- ja puolustusasiain komitea (TPaK).

Tietoturvallisuustoimien tavoitteena on hyvän tiedonhallintatavan ja asianmukaisen tietoturvallisuuden perustason luominen myös poikkeusolojen aikaisen tiedonkäsittelytoiminnan varmistamiseksi.⁹ Tämän vuoksi organisaation on laadittava tietoturvallisuusanalyysi, määriteltävä tarvittavat toimenpiteet ja annettava ohjeet oman organisaation ja hankkimiensa palvelujen tietoturvallisuudesta. Tietoturvallisuuden kehittämistä ohjaa valtionhallinnon tietoturvallisuuden johtoryhmä valtiovarainministeriössä (VAHTI). Valtionhallinnon ja kunnallishallinnon tietohallintoyhteistyön yhteistyö- ja neuvotteluelimenä on sisäasiainministeriön yhteydessä julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA).

Poikkeusoloihin varautumisessa kokonaisvastuu maan taloudellisesta turvallisuudesta sekä väestön toimeentulon että talouselämän turvaamisesta kuuluu valtion ylimmälle johdolle ja viranomaisille, joilla on toimivalta näillä alueilla normaaliaikanaan. Valtioneuvosto sekä kukin ministeriö omalla hallinnonalallaan johtaa, valvoo ja yhteen sovittaa poikkeusoloihin varautumista.¹

Viranomaisen, valtion liikelaitosten sekä kuntien tulee valmiussuunnitelmin ja poikkeusolojen toiminnan etukäteisvalmisteluin sekä muin toimin varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa. Suunnittelussa otetaan huomioon valtiovarainministeriön (VM) tärkeysluokitus toiminnan ja tietojenkäsittelyn merkityksen mukaan.

Julkisoikeudellisia laitoksia koskevat soveltuvin osin edellä mainitut valtion laitoksia koskevat velvoitteet.

Kunnilla on vastuu tietojärjestelmiensä kehittamisestä ja ylläpidosta. Riittävän tietoturvallisuuden saavuttamiseksi kuntien on laadittava oma tietoturvallisuussuunnitelmansa, jossa eri toimijoiden vastuut ja velvollisuudet määritellään. Valtionhallinnon tietoturvallisuusohjeistoja voidaan soveltuvin osin hyödyntää kunnan tietoturvallisuussuunnitelman laadintaan. Valmiussuunnittelussa otetaan huomioon lääninhallitusten ohjeet. Suomen Kuntaliitto on valmistellut suosituksia, joita kunnat voivat käyttää tietohallintonsa turvallisuuden ja valmiuden kehittämisen apuna. Kuntayhtymää sekä kunnallista laitosta koskee soveltuvin osin kunnan velvoite.¹

3. TIETOJENKÄSITTELYN VARMISTAMINEN JOHTAMISEN OSANA

3.1 Johtaminen ja toiminnan jatkuvuus

Tietoturvaluuutta ja valmiutta sekä niiden hoidon vastuuta on tarkasteltava toiminnan näkökulmasta. Tietoturvaluuustarpeet lähtevät käyttäjäyksiköistä. Toimintavastuun hajauttaminen yksiköihin on ohjannut myös tietoturvaluuden suunnittelun toimintojen vastuuhenkilöille ja tietojärjestelmien omistajille. Tietotekninen henkilöstö ei voi tuntea riittävän hyvin palveluiden ja toimintojen tietoturvaluus- ja valmiusvaatimuksia. Jos johto, toimintojen vastuuhenkilöt ja tietojärjestelmien omistajat eivät osallistu turvaluuden määrittelyyn, tietoturvaluuteen voi jäädä puutteita, joita ei tunneta ja joista kukaan ei ota vastuuta.

Tietoturvaluus kuuluu nykyaikaiseen johtamiseen. Sen tulee sisältyä jokaisen johtotehtävissä toimivan henkilön vastuisiin. Tietoturvaluus toteutuu parhaiten suunnitteluprosessien, laatujärjestelmien ja tavanomaisen toiminnan tavoitteiden kiinteänä osana. Ylimmän johdon tulee vahvistaa periaatteet tietoturvaluuden johtamisesta, suunnittelusta, toimeenpanosta ja varautumisesta poikkeusoloihin. Johto vastaa organisaationsa turvaluusstietoisuudesta sekä ohjaa näkemään ja arvioimaan toimintaa vaarantavia tekijöitä.

Yksiköissä tietoturvaluusvastuut ovat toimintovastuun osa. Yksiköiden johdolla on parhaat edellytykset asettaa vaatimukset tietoturvaluudelle, koska se tuntee tietojenkäsittelyn riippuvuudet sekä yhteiskunnan, sidosryhmien, asiakkaiden ja yhteistyökumppanien odotukset palvelujen ja toiminnan osalta. Tietoturvaluusvastuut nimetään tehtäväkohtaisesti johtamiskäytännön mukaisesti. Yksiköiden esimiehet vastaavat tietoturvaluuden ja valmiuden toteutumisesta sekä valvonnasta tulosvastuun periaatteiden mukaisesti. Tietoturvaluusvastuun tulee seurata organisaation ja toiminnan muutoksia.

Organisaation tietoturvaluuden kokonaisvaltainen kehittäminen, valmistelu ja ohjaaminen vaativat usein keskeisten tehtävien osoittamista erikseen nimetyille vastuuhenkilöille tai päätoimiselle tietoturvaluuden vastuuhenkilölle.

Tietoturvaluuden vastuu- ja tehtäväjaosta on esimerkki liitteessä 4a tietoturvaluusvastuut ja tehtäväjako.

3.2 Tietoturvaluuspolitiikka

Tietoturvaluuspolitiikka on välttämätön lähtökohta tietoturvaluuden ja valmiuden kehittämiselle organisaatiossa. Sen avulla ylin johto määrittelee tietoturvaluuden periaatteet ja toimintatavat sekä ohjaa tietoturvaluuden huomioon ottamista, suunnittelua ja toimeenpanoa organisaation eri tasoilla.

Tietoturvallisuuspolitiikka (esimerkki)

Sisältö

- tietoturvallisuuden tarkoitus, tavoitteet
- keskeisillä toimialoilla ja tehtävissä noudatettavat tietoturvallisuuden periaatteet
- keskeisiä toimintoja tukevien toimintojen tietoturvallisuusperiaatteet
- käytettävien teknisten järjestelmien tietoturvallisuusperiaatteet
- organisaatio ja tietoturvallisuusvastuut
- toteutustapa ja tietoturvallisuuden linjaukset
- ohjeet ja koulutus
- seurannan järjestely – valvonta ja raportointi
- erikoisalueet: mm. tuotanto, palvelut ja sähköiset palvelut
- ulkoistettujen palvelujen tietoturvallisuus
- tietoturvallisuus laite-, ohjelmisto- ja tietojärjestelmähankkeissa sekä kehitystyössä
- kriittisten tietovarastojen suojaus, dokumentointi ja järjestelmäkuvaukset
- tarvittavat suunnitelmat ja ohjeet
- periaatteet elintärkeiden toimintojen varmistamiseksi vakavissa keskeytystilanteissa
- periaatteet poikkeusolojen valmiudelle.

Turvallisuuspolitiikassa määritellään myös jatkuvuuden varmistaminen ja varautuminen poikkeusoloihin tärkeysluokituksen mukaisesti. Tietoturvallisuuspolitiikkaan sisältyvät periaatteet ovat toiminnasta lähteviä vaatimuksia ja järjestelmistä ja teknisistä toteutustavoista riippumattomia.

3.3 Toiminnan suunnittelu

Johdon päätöksiin perustuvat tietoturvallisuuden tehtävät sisällytetään vuosittain toimiala-, yksikkö- ja tietojärjestelmäkohtaisiin kehittämissuunnitelmiin sekä hankintoihin.

Tietojärjestelmillä on palvelukyvyyn kannalta usein selvästi strateginen merkitys. Vastaavasti toiminnan jatkuvuutta varmistavat tietoturvallisuusratkaisut ovat strategisesti tärkeitä ja tietohallintostrategiaan sisällytettäviä.

Tietoturvallisuuden ohjaus ja suunnittelu

| Konsernitaso | Toimialaryhmät | Liiketoimintayksiköt |
|--|--|--|
| Johtaminen | | |
| Tietoturvallisuus <ul style="list-style-type: none">• politiikka• ohjaus• resurssit• sähköposti ja muut konsernitason järjestelmät• valvonta | Periaatteet <ul style="list-style-type: none">• perusturvallisuus• poikkeusolojen valmiussuunnitelmat | Tietoturvallisuussuunnitelmat <ul style="list-style-type: none">• operatiiviset tietojärjestelmät• operatiiviset tietovarastot• prosessipohjaiset tietoturvallisuussuunnitelmat Toipumissuunnitelmat |
| Ylläpito | | |

Strategisten päätösten ja suunnitelmien vaikutukset tietoturvallisuuteen tu-

lee tarkistaa mm. muutettaessa toimintalinjauksia tai otettaessa käyttöön uusia sähköisiä palveluja.

Tietoriskit ja niiden hallinta organisaatiossa sisällytetään myös riskienhallinnan kokonaissuunnitelmiin.

3.4 Tietojärjestelmien luokitus

Tietoturvallisuus-, toipumis- ja valmiusvaatimuksia voidaan kohdentaa tietojärjestelmien luokituksella.

Normaalioloissa tietojärjestelmien luokituksen perustana on niiden merkitys toiminnalle sekä palvelutaso- ja laatuvaatimukset. Poikkeusoloissa luokitus voi olla toisenlainen.

Normaalioloissa:

1. ryhmään kuuluvat tärkeät tietojärjestelmät, joiden tietoturvallisuuden ja toipumisvalmiuden on oltava korkealla tasolla. Näitä ovat esimerkiksi logistiikkajärjestelmät, tuotannon ohjaus, palveluketjut, tärkeät tietovarastot sekä valtakunnallisesti tärkeät ja muut keskeiset hallinnon järjestelmät ja sähköposti.

2. ryhmään kuuluu yrityksen sisäisille toimintaedellytyksille tärkeitä tietojärjestelmiä, kuten taloushallinto, asiakaspalvelujärjestelmät sekä johdon informaatiojärjestelmät, joiden käytettävyys normaalioloissa tulee varmistaa.

3. ryhmään kuuluvat sellaiset tietojärjestelmät, joissa tilapäinen keskeytyminen ei aiheuta välittömiä vahinkoja. Näitä ovat esimerkiksi henkilöstöhallinnon, suunnittelun ja markkinoinnin järjestelmät sekä tilastointi.

Vaatimukset eritellään tietojärjestelmittäin. Palvelutasoa voidaan mitata esimerkiksi suurimmalla sallitulla keskeytyksellä ja käyttötavan määrittelyllä.

Poikkeusolojen kriittisten tietojärjestelmien luokitusta on käsitelty poikkeusolojen valmiussuunnittelun yhteydessä.

3.5 Tietoturvallisuus hankinnoissa

Palvelu-, laitteisto- ja ohjelmistohankinnat

Palvelusopimuksissa sekä laitteisto- ja ohjelmistohankintojen yhteydessä voidaan ratkaisevasti vaikuttaa tietoturvallisuuteen ja valmiuden kehittämiseen selvittämällä ennen hankintaa palveluihin ja tuotteisiin liittyvät turvallisuusvaatimukset ja palveluyrityksen tietoturvallisuuspalvelujen toimituskyky.

Hankintojen yhteydessä tarkasteltavia tekijöitä ovat:

- turvallisuusvaatimukset palveluille
- järjestelmähallinta, ohjelmistojen tarjoamat turvallisuusominaisuudet ja valvontamenettelyt, eheys, luottamuksellisuus, käytettävyys, todennus ja kiistämättömyys
- riittävän yhtenäisen, korvaavan laitekannan ja käyttöjärjestelmien yhteensopivuuden luominen

- palvelu-, huolto-, laite- ja ohjelmistotoimittajien osaaminen ja voimavarat
- nopean huollon ja varaosapalvelujen varmistaminen
- varalaitteiden saatavuuden varmistaminen sopimuksissa.

Merkittävien järjestelmähankintojen yhteydessä varmistetaan laite-, ohjelmisto- ja tukipalveluyrityksen mahdollisuudet toimituksiin myös poikkeusoloissa.

Järjestelmäkehitys

Tietoturvallisuus on järjestelmäkehityksen tärkeä osa-alue. Järjestelmäkehityksen yhteydessä tarkasteltavia turvallisuustekijöitä ovat:

- kehitysvaiheen turvallisuustehtävät
 - kehitettävänä olevaan tietojärjestelmään kohdistuvien tietoriskien arviointi ja sen tukemien palvelujen elintärkeys ja valmiusvaatimukset yhteiskunnan kannalta
 - turvallisuusvaatimusten ja –tason määrittely
 - tietojärjestelmähankkeen tietoturvallisuusvastuiden järjestely
 - tietojärjestelmäprojektin tietoturvallisuus
- määrittelyvaiheen tietoturvaluustehtävät
 - ratkaisuperiaatteet
 - tietoturvaluustechnikat ja –ominaisuudet
 - laadunvarmistusmenettelyt tietoturvaluuden kannalta (eheys, luotamuksellisuus, käytettävyys, todentaminen, kiistämättömyys)
- toteutusvaiheen turvallisuustehtävät
 - tietoturvaluusratkaisujen toteutus
 - tietoturvaluusmenettelyjen testaus ja hyväksyminen käyttöön tietojärjestelmän käyttööntovaiheessa
- käytön tietoturvaluustehtävät
 - järjestelmän käytön ja ylläpidon tietoturvaluusvastuuhenkilön nimeäminen ja tehtävämäärittelyt
 - tarvittavan tietoturvaluuskoulutuksen antaminen ja ohjeiston käyttöönotto
 - tietoturvaluuden ylläpito ja käyttöturvaluudesta huolehtiminen käyttöympäristössä
 - tietoturvaluuden seuranta ja valvonta sekä raportointi tietojärjestelmän omistajalle
 - version päivityksen tietoturvaluustehtävät
- testaus ja laadunvarmistus
- varmuus- ja suojakopiointijärjestelyt, tallennustiheys, käyttöönotto, testaus
- varajärjestelmätarpeet.

3.6 Tietoturvaluus ja laatu

Tietoturvaluus ja laatu liittyvät monella tavoin yhteen. Tietoturvaluudella on suuri merkitys organisaation tietotekniikasta riippuvan toiminnan laadullisena varmistajana. Käytännössä tämä tarkoittaa tietoturvaluuden huomioon ottamista laatujärjestelmissä tuotannon ja palvelujen turvaamiseksi ja varmistamiseksi. Käytettävien tietojärjestelmien on si-

sällettävä palvelutason edellyttämät turvallisuusmenettelyt. Tietoturvallisuusmenettelyjen on täytettävä tietoturvallisuuden laatukriteerit. Myös tietoturvallisuuden laatuajattelussa asiakkaiden tarpeet ja palvelukyky ovat keskeisiä tavoitteita.

Laatujärjestelmästä tietoturvallisuuteen kohdistuvia vaatimuksia

Johtajuus

Tietoturvallisuuden johtamiskäytäntö

Toimintaperiaatteet ja strategia

Turvallisuuspolitiikka, tietoturvallisuuspolitiikka ja turvallisuus toimintastrategioissa sekä näiden muuttaminen toiminnaksi

Henkilöstö

Tietoturvallisuuden osaaminen ja sen sisällyttäminen toimintatapoihin

Yhteistyökumppanuudet ja resurssit

Tietoturvallisuuden hallinta yhteistyösuhteissa, teknologiassa, tiedon ja tietämyksen hallinnassa sekä fyysisen toimintaympäristön hallinnassa

Ulkoistaminen ja turvallisuuden hallinta

Palvelujen hankinnan tietoturvallisuus

Prosessien hallinta

Tietoturvallisuuden hallinta prosessien kehittämisen, suunnittelun ja järjestelmähallinnan osana omassa ja yhteistyökumppaneihin liittyvissä prosesseissa sekä tietoturvallisuuden prosessien jatkuva kehittäminen

Asiakastulokset

Tietoturvallisuuden mittarit ja tulosten seuranta asiakkaiden ja suorituskyvyn näkökulmista

Henkilöstötulokset

Motivaatio, tyytyväisyys ja suorituskyky, tietoturvallisuustyön osaaminen, sitoutuminen

Yhteiskunnalliset tulokset

Vastuu yhteiskunnan toimivuudesta

Turvallisen kehityksen seuraaminen

Turvallisuutta vaarantavien tapahtumien havainnointi ja niihin ennalta vaikuttaminen

Uusien tietojärjestelmien ja niihin perustuvien palvelujen tietoturvallisuus ja laatu luodaan järjestelmäkehityksen yhteydessä. Useimmiten se on myöhemmin tehtynä joko hyvin kallista tai mahdotonta.

Turvallisuusvaatimuksia on jo jonkin aikaa käsitelty laatustandardeissa. ISO IS 15408 ja englantilainen BS 7799 ovat eräitä tietoturvallisuuden laatujärjestelmän standardeja. Sertifioitavalla yrityksellä tulee olla tietoturvallisuuspolitiikka ja selkeät turvallisuustavoitteet, joissa otetaan huomioon myös yhteiskunnan asettamat velvoitteet. Standardia voidaan soveltaa yksityiskohtaiseen tietoturvallisuuden laadun kehittämiseen liitettynä koko organisaation laatujärjestelmään. Standardin ohella on kuitenkin otettava huomioon mm. poikkeusolojen valmiudelle asetetut vaatimukset ja velvoitteet sekä muut määräykset. Erityisesti kriittisten tietojärjestelmien ja ohjelmistojen sekä turvallisuusohjelmistojen ja –menettelyjen laatuarviointi on välttämätöntä. Standardien ohella on tietoturvallisuuden arviointiin ja kehittämiseen kansainvälisesti ja EU:n piirissä luotu normeja kuten tietotekniikan turvallisuuden arvioinnin käsikirja ITSEM (Information Technology Security Evaluation Manual, EU) sekä tietojärjestelmien turvallisuuden arviointivaatimukset ITSEC (Information Technology Security Evaluation Criteria) ja TCSEC (Trustee Computer System Evaluation Criteria).

3.7 Ohjeet

Tietohallinnossa ja yksiköissä tarvitaan ohjeita turvallisuustoimien toteuttamiseksi pysyvällä ja tietoturvallisuusperiaatteisiin pohjautuvalla tavalla. Esimerkiksi VM on laatinut valtionhallinnon yksiköille tietoturvallisuusohjeet, joista useimmat sopivat myös yritysten ohjeiston perustaksi.

Tärkeimmät valtionhallinnon ja PTS:n ohjeet on esitetty liitteessä 3.

4. UHAT JA HAAVOITTUVUUDEN ARVIOINTI

4.1 Tietotekniikan riskit sekä niiden vaikutus toimintaan

Verkottuminen saa aikaan uusia riskejä ja lisää vahinkojen todennäköisyyttä ja laajuutta. Tietojenkäsittelyn haavoittuvuus kasvaa. Erityisesti riskialttiutta ja turvallisuustarpeita lisää turvallisuudeltaan puutteellisten avoimien verkkojen kuten Internetin käyttö. Laajat verkkoihin hajautetut tietojärjestelmät kohottavat järjestelmähallinnan vaatimuksia tiedon säilyttämiseksi ja suojaamiseksi sekä käytettävyyden, oikeellisuuden ja luotettavuuden varmistamiseksi. Verkkopalvelujen vuorovaikutteisuus moninkertaistaa tietojärjestelmissä olevan suojattavan tiedon määrän sekä synnyttää laajoissa järjestelmissä testaamattomia tilanteita. Tiedon jakelu verkoissa parantaa tiedon saatavuutta mutta se lisää pääsynvalvonnan ja tiedon hallinnan vaatimuksia.

Järjestelmäkehityksen nopeus vähentää testausten määrää. Ohjelmistot ovat avoimia. Niiden suojausominaisuudet kehittyvät hitaammin kuin käyttöominaisuudet. Vanhoista järjestelmistä ja järjestelmien osista puuttuvat suojaukset. Nopea laitteiden ja ohjelmistojen uusiutuminen vähentää yhteensopivuutta vaikeuttaen järjestelmien hallintaa. Laite- ja ohjelmistotoimitukset sekä tukipalvelut keskittyvät osaaville palvelujen tuottajille. Perinteisiä manuaalijärjestelmiä ei usein enää ole. Niihin palaaminen korvaavina järjestelminä ei ole mahdollista ilman erityisiä toimenpiteitä. Siten tietotekniikan toimivuus- ja varajärjestelmävaatimukset kasvavat.

Palvelujen ulkoistamisen seurauksena turvallisuusvaatimusten asettaminen ja turvallisuuden valvonta vaikeutuvat. Oma henkilöstö tarvitsee yhä perusteellisempaa tietoturvallisuuskoulutusta. Poikkeusolojen valmiuden ylläpitäminen edellyttää sopimuksia palveluyritysten kanssa.

Tietojenkäsittelyn turvallisuuden tarpeeseen vaikuttavat myös muutokset yhteiskunnassa. Luvattomia vaikutuskeinoja hakevien henkilöiden ja ristiiriitaryhmien lisääntyvä toiminta liittyneenä tietotekniikan osaamiseen ja työttömyyden aiheuttamaan turhautumiseen on huomionarvoinen uhka. Vakavat hyökkäykset kansallisesti ja kansainvälisesti tärkeisiin tietojärjestelmiin ja niihin kohdistuva terrori ovat mahdollisia. Kansainvälisen riippuvuuden seurauksena keskeytyksistä aiheutuvat vahingot voivat olla laajoja.

Riippuvuus ulkomaisista tietotekniikka- ja verkkopalveluista, tiedonsiirosta sekä laite-, varaosa- ja tukipalveluista on merkittävä haavoittuvuusriski. Erityisesti poikkeusoloissa tästä seuraa tietojenkäsittelylle vakavia ongelmia.

Haavoittuvuus kasvaa nopeasti ellei turvallisuutta kehitetä organisaation toiminnan ja tietojenkäsittelyn osana. Turvallisuus on tietotekniikan jatkuvan kehittämisen edellytys. Uusia, avoimia tietotekniikkaratkaisuja ei voida rakentaa turvallisuudeltaan puutteellisten perusjärjestelmien varaan.

4.2 Sisäiset ja ulkoiset uhat

Normaaliin toimintaan kohdistuvat uhat

Normaaliin toimintaan kohdistuvien uhkien syinä ovat usein puutteet tietoturvallisuuden hallinnollisissa menettelyissä kuten toimintaperiaatteissa ja ohjeissa, henkilöstön aiheuttamat tahattomat tai tahalliset häiriöt, laitteiden ja ohjelmistojen viat ja puutteet, fyysisen turvallisuuden puutteet sekä puutteet poikkeavien tapahtumien havainnoinnissa ja käytön valvonnassa.

Puutteellisesta turvallisuudesta aiheutuvat vahingot voivat muuttua laajoissa ja aroissa järjestelmissä vakaviksi vaurioiksi, keskeytyksiksi ja mittaviksi taloudellisiksi menetyksiksi.

Tällaisia vahinkoja ovat esimerkiksi:

- logistiikkaketjujen menetys
- tietovarastojen ja niiden eheyden menetykset
- käytettävyyden lasku, häiriöt palveluissa ja tuotannossa
- virheet tietojen ja tuotteiden laadussa
- tietosuojan rikkoutuminen
- kilpailuedun menetys, luotettavuuden heikkeneminen
- työmotivaation lasku
- keskitettyjen resurssien - palvelimien, verkkoajan, nimi- ja hakemistopalvelujen ja järjestelmän osien - häiriöiden laajalle ulottuvat vaikutukset.

Toiminnan jatkuvuuteen kohdistuvat uhat

Tietojärjestelmien hyödyllisyys riippuu tänä päivänä tietoverkkojen toimivuudesta. Käytännössä tietojärjestelmän voi muodostaa laaja tietoverkko laitteistoineen. Verkkojen toimintaa ja luotettavuutta häiritsevät niiden eri osissa esiintyvät viat sekä puutteet ja vaikeudet verkon varmistamisessa. Normaalioloissa edellytetään verkkojen yhtämittaista käytettävyyttä. Varmistaminen vaatii yhteistyötä palveluyritysten, verkko-operaattorien ja muiden yhteistyötahojen kanssa.

Palveluverkkojen ja laajojen tietojärjestelmien avainkohdissa sattuneet keskeytykset voivat muodostua vaikeiksi, ellei elintärkeitä tietojärjestelmiä ole varmistettu. Oman toiminnan ohella keskeytykset vahingoittavat asiakkaiden toimintaa ja heikentävät luotettavuuskuvaa.

Riskeinä ovat:

- elintärkeiden järjestelmien vakava käytön keskeytyminen, tietojen menetys ja vakavat vahingot koko järjestelmässä sekä palvelujen, tuotannon ja toimitusten keskeytyminen
- tuottojen väheneminen, rahavirran katkeaminen
- viivästymiset ja niiden aiheuttamat taloudelliset menetykset
- lisääntyneet kustannukset, sopimussakot ja korkomenetykset
- menetetyt tilaukset
- palvelujen, tuotannon ja toimituksien estyminen, asiakkaiden palvelutason lasku
- yrityskuva- ja asiakasmenetykset
- toiminnan jatkamisen kannalta muut kriittiset menetykset.

Tietoturvallisuustoimenpitein voidaan olennaisesti vähentää keskeytyksiä aiheuttavien riskien todennäköisyyttä ja rajata vahinkoja. Valmius elintärkeiden järjestelmien varajärjestelmiin sekä normaalitoimintaan palaamiseen varmistaa elintärkeän toiminnan lyhentäen keskeytysaikaa ja vähentäen käyttäjille ja asiakkaille syntyviä vahinkoja.

Erityistilanteet

Yleisesti erikoistuminen ja toimintojen keskittyminen, verkottuminen ja tukeutuminen yhtämittaista toimintaa vaativiin järjestelmiin johtaa jo normaalioloissa joillakin toimialoilla toimialakohtaisiin ongelmiin. Tietotekniikka on tällainen toimiala. Organisaation omasta toiminnasta riippumatta saattaa tietojenkäsittelyyn kohdistua ulkopuolelta sellaisia häiriöitä ja keskeytyksiä, jotka aiheutuvat tietotekniikan perusrakenteiden rikkoutumisesta ja johtavat erityistilanteisiin.

Erityistilanteiden seurauksia ovat mm.:

- kansainvälisten verkkojen yli hoidettavien palvelujen ja asiakaspalvelujen, jatkuvien asiakasyhteyksien sekä verkon yli tapahtuvien ylläpito- ja huoltopalvelujen keskeytyminen
- sähköpostiyhteyksien menetys
- tietovarastojen haavoittuminen sekä muut eheyden ja käytettävyyden menetykset.

Varautuminen uudenaikaisiin, laajavaikutteisiin erityistilanteisiin edellyttää toipumissuunnittelua. On huomattava, että varautuminen erityistilanteisiin ei koske vain tärkeyslukiteltuja organisaatioita vaan on tarpeen kaikissa merkittävästi tietotekniikkaa ja verkkoja hyödyntävissä organisaatioissa.

Poikkeusolojen tietojenkäsittelyyn kohdistuvat uhat

Poikkeusoloissa organisaatioiden toimintaan vaikuttavat poikkeusolojen muuttunut toimintaympäristö ja toimintaedellytysten kaventuminen.

Tietojenkäsittelylle tyypillisiä uhkia ovat yhteyksien katkeamiset, tietojärjestelmien käytön estyminen, resurssien väheneminen sekä ylläpidettävien toimintojen uudelleenjärjestäminen. Poikkeusoloissa verkkojen toimintavarmuuden ja siitä riippuvan huoltovarmuuden turvaaminen on ongelmallista.

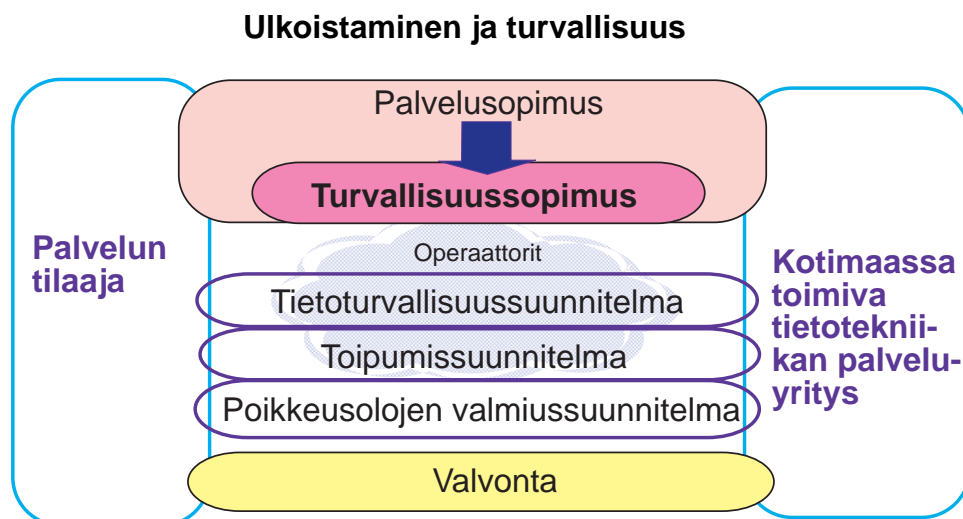
Poikkeusolojen vaikutuksia ovat:

- organisaation omien toimintaedellytysten lasku tai menetys
- hallinnon ja talouselämän tietojärjestelmien ja tiedonsiirron lamautuminen
- toimeentuloon vaikuttavien tietojärjestelmien, laajojen palvelu-, maksuliikenne-, ohjaus- ja tietokantajärjestelmien lamautuminen ja huoltovarmuuden vaarantuminen
- normaaliolojen tietojenkäsittelyn laajamittainen alasajo ja siirtyminen poikkeusolojen tuotantoon ja sen tietojärjestelmiin valmiussuunnitelmien mukaisesti.

Poikkeusolojen valmiussuunnittelussa on selvittävä verkkopalvelujen, tietoliikenneyhteyksien ja perusrakenteiden toiminnan keskeytysten vaikutus. Varautumistoimenpiteet ovat luonteeltaan edellä kuvattujen normaaliolojen erityistilanteiden kaltaisia. Poikkeusoloissa vaikutusalue on kuitenkin laajempi ja keskeytykset pitkäaikaisempia.

4.3 Ulkoistaminen ja turvallisuus, tietotekniikan palveluyrityksen valmius

Ulkoistettujen tietotekniikkapalveluiden tietoturvallisuudesta ja poikkeusolojen valmiudesta vastaa sama taho, joka vastaa ulkoistamisestakin. Tietoturvallisuuden ja jatkuvuuden sekä tarvittaessa poikkeusolojen valmiuden vaatimukset ulotetaan ulkoistettuihin palveluihin ja palveluyritykseen. Tämä edellyttää palvelun ulkoistajan ja palvelun toimittajan välisten velvoitteiden jakoa, tehtävämäärittelyä ja tietoturvaluussuunnitelmaa, jotta haluttu tietoturvallisuuden taso saavutetaan ja säilytetään. Osan turvallisuustehtävistä voi hoitaa vain yritys itse mutta osaan tarvitaan välttämättä palveluyrityksen apua.



Tietotekniikan palveluyrityksen tulee valmiussuunnitelmaa laatiessaan tietää asiakkaansa valmiusvaatimuksista. Vaatimukset tulee käsitellä jo palvelusopimusta tehtäessä ja sisällyttää tarvittavassa laajuudessa palvelusopimukseen tai erilliseen turvallisuussopimukseen. Palvelun tilaajan tulee valvoa valmiuden toteutumista.

Ulkoistajan tulee varmistaa toipumissuunnittelun yhteydessä, miten palveluyritys huolehtii samanaikaisesti eri asiakkaidensa varajärjestelmän käytöstä ja käynnistyksestä.

Ulkoistamisen yhteydessä ja turvallisuussopimusta tai -suunnitelmia laadittaessa selvittäviä ja sovittavia seikkoja ovat:

- käyttöhenkilöstön valinta ja hallinta
- turvallisuustapahtumien ja rikkomusten raportointi toimeksiantajalle
- toimeksiantajan yhteyshenkilöiden ja heidän toimintavaltuuksiensa toteaminen

- turvallisuustoimenpiteiden ja häiriöiden seuranta sekä mittaaminen esimerkiksi laatuyhteistyöhön liittyen
- toimeksiantajan oikeus tarkastaa turvallisuustoimenpiteiden tasoa
- palveluyrityksen kyky hoitaa tietojenkäsittelyn varmistaminen poikkeusoloissa.

Ulkoistamisen tietoturvaluustoimet eivät koske ainoastaan tietotekniikkapalvelujen toimittajia vaan myös muita erilaisten suunnittelu-, tuotanto-, toimisto- ja huoltopalvelujen tuottajia. Palvelujen yhteydessä on palvelujen sisällöstä riippuen tarkistettava tietoturvaluustarpeet ja laadittava salassapitosopimus tai tarvittaessa turvallisuussopimus.

Ulkoistamisen yhteydessä on myös varmistettava, ettei palvelun toimittajalle luovuteta sellaisia tietoja tai pääsyä sellaisiin tietoihin, joita salassapitomääräysten vuoksi ei voida luovuttaa ulkopuolisten käyttöön.

4.4 Sähköiset palvelut ja turvallisuus

Hyvä tiedonhallinta ja tietoturvaluisuus

Laissa viranomaisen toiminnan julkisuudesta ja henkilötietolaissa edellytetään valtion viranomaisten ja muidenkin valtionhallinnon organisaatioiden noudattavan hyvää tiedonhallintatapaa tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisen saatavuuden ja käytettävyyden varmistamiseksi ja suojaamiseksi sekä eheyden ja muiden laatuun vaikuttavien tekijöiden hoitamiseksi.

Hyvän tiedonhallintatavan tunnusmerkkejä ovat:

- tiedonhallinnan asianmukainen resurssointi ja organisointi
- toiminnan varmistava ohjeistus
- suunnitelmallisuus, huolellisuus, luottamuksellisuus ja lainmukaisuus
- ajan tasalla ylläpidettävät kuvaukset tietoprosessien ja tiedonhallinnan tehtävistä, aineistoista sekä niiden käsittelystä, salassapidosta ja hävittämisestä
- käsiteltyjen tietojen luettelointi
- tietoturvaluisuuden sisältyminen olemassa olevaan ohjejärjestelmään ja laatujärjestelmään.

Hyvään tiedonhallintatapaan kuuluu erottamattomasti tietoturvaluisuus. Tietoturvaluustoimenpiteillä voidaan varmistaa hyvän tiedonhallintatavan toteutuminen.

Internetin tietoturvaluisuus

Internet on sähköisen liiketoiminnan ja lukuisien keskeisten palvelujen keskus ja yhteysväline organisaation ja sen asiakkaiden välillä sekä kotimaassa että kansainvälisesti.

Internet, intranet ja ekstranet muodostavat käytännössä yhtenäisen kokonaisuuden, jossa käytetään Internetin tekniikkaa ja noudatetaan sen käyttötapoja. Myös verkoissa toimivien logistiikka- ja palveluketjujen turvallisuutta ja käytettävyyttä on tarkasteltava kokonaisuutena. Näiden ketjujen yhteydet muodostetaan pääasiassa teleoperaattoreiden virtuaaliverkkoina.

Internetin tietoturvaluossuosituksia on VM:n ohjeessa Valtion Internetin käyttö- ja tietoturvaluossuositus sekä PTS:n selvityksessä Internet, toiminnan verkottuminen ja sen haavoittuvuus. Turvullisuusriskejä käsittelee PTS:n julkaisema Selvitys Internetin turvullisuusriskeistä.¹⁰ Valtion periaatteet velvoittavat myös julkishallinnon tietoja käsitteleviä ulkopuolisia tahoja.

Kuten tietoverkoissa yleensä, tulee erityisesti Internetissä huolehtia käsiteltävien tietojen eheydestä, luottamuksellisuudesta ja käytettävyydestä sekä todentamisesta ja kiistämättömyydestä. Palveluita, joiden tietoturvaluossuutta ei Internetissä voida taata, ei myöskään pidä siinä tarjota.

Internetiin kytkeytyneiden organisaatioiden välinen tietoliikenne voidaan toteuttaa edellyttäen, että osapuolet noudattavat samoja tietoturvaluossuperiaatteita tunnituksessa, tietoliikenteen salauksessa ja käytettävyyden ylläpidossa. Internetin käyttöperiaatteet, ehdot ja vaatimukset tulee määrittellä organisaatiokohtaisesti turvullisuuspolitiikassa.

Poikkeusolojen kannalta on tarkasteltava sekä kokonaisuutta että yksittäisten verkkojen käytettävyyttä ja varmistamista poikkeusoloissa. Internetin lamautuminen pysäyttää osan yritysten ja yhteiskunnan toiminnasta.

Sähköposti

Sähköpostin tietoturvaluossuuden tarkoituksena on sähköpostipalvelun ja –asioinnin suojaaminen niin, etteivät ulkopuoliset pääse käyttäjien salasanoihin eikä sähköpostitiedostoihin sekä itse järjestelmän turvullisuuden ja käytettävyyden varmistaminen.

Sähköposti on organisaatioiden viestinnän tärkein palvelu. Sen käytön estyminen turvullisuuden puutteiden, häiriöiden ja tahallisen sabotoinnin seurauksena voi vakavasti vaikeuttaa johtamista ja tiedonvälitystä sekä estää samalla muita toimia. Sähköpostin käyttöön liittyy erityisiä eheys-, luottamuksellisuus- ja käytettävyyssriskejä. Suojaamaton sähköposti on altis postitalaisuuden loukkauksille. Sähköpostia ei voida käyttää ottamatta huomioon näitä riskejä. Sähköpostin toiminnan varmistaa nopeasti käyttöön otettava, valmisteltu varajärjestelmä.

Sähköpostin tietoturvaluossuuteen kohdistuvat rikoslain säädökset oikeudettomasta puuttumisesta toisten viesteihin ja henkilötietolain säädökset henkilötietojen käsittelystä. Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvaluossusta koskee televiestinnän luottamuksellisuutta, salassapitovelvollisuutta ja hyväksikäyttökieltoa. Laissa viranomaisen toiminnan julkisuudesta annetut säädökset koskevat viranomaisen tietojen ja asiakirjojen salassapitoa ja käsittelyä.

Laissa yksityisyyden suojasta työelämässä¹¹ sähköpostin ja tietoverkon käyttö kuuluvat yhteistoiminnasta yrityksissä annetussa laissa sekä yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa tarkoitettun yhteistoimintamenettelyn piiriin.

Sähköpostin käytön tulee perustua johdon vahvistamiin periaatteisiin mm. työntekijän henkilökohtaisen postiosoitteen käytöstä, yrityksen postien ohjaamisesta sekä valvonnasta yksityisyyttä loukkaamatta.

Sähköpostin käyttö- ja valvontaperiaatteet määritellään tietoturvallisuuspolitiikassa. Periaatteiden on oltava koko henkilöstön tiedossa. Mikäli työnantaja sallii sähköpostin käytön henkilökohtaisessa viestinnässä, johdon on selvítettävä turvallisuustekijät ja päätettävä käytön rajoituksista.

Varsinkaan poikkeusoloissa ei voida tukeutua organisaation oman verkon ulkopuolella toimiviin sähköpostijärjestelmiin, joten yhteydet on varmistettava vaihtoehtoisin menetelmin.

Sähköinen kaupankäynti ja palvelujen turvallisuus

Sähköisen kaupankäynnin ja palvelujen tuottajan tulee huolehtia tietoturvallisuudesta ja palvelun varmistamisesta. Tietoturvallisuuden kannalta tärkeimpiä ovat sähköinen tunnistus ja allekirjoitus sekä kiistämättömyys (sähköisten palveluiden ja asiointin tietoturvallisuuden yleisohje, VAHTI 4/2001).

Sähköiset palvelut edellyttävät yhtenäisiä turvallisuusperiaatteita. Vastuu sähköisten palvelujen tietoturvallisuudesta on määriteltävä palvelun kehittämisestä ja ylläpidosta vastaavalle taholle.

Poikkeusoloissa sähköisten palvelujen käytettävyyttä ei voida taata, eikä sähköisen tunnistuksen varmennepalveluja kyetä hoitamaan luotettavasti.

Salaus

Salaus on menettely, jolla tieto muutetaan tarkoituksella salatuksi, varmistetaan sen aitous estäen huomaamaton muuttaminen ja ehkäistään valtuuteton käyttö. Salaus on tärkeä keino siirrettävän tai säilytettävän tiedon suojaamiseen. Salauksella nostetaan ratkaisevasti eheyden, luottamuksellisuuden, käytettävyyden, todentamisen sekä kiistämättömyyden tasoa.

Tietoturvallisuuden parantamiseksi salausta tarvitaan:

- käyttäjän todentamisessa
- sähköpostissa ja siirrettävien tietoaineistojen turvaamisessa
- säilytettävän tietoaineiston suojaamisessa
- työasemien ja erityisesti kannettavien tietokoneiden kiintolevyjen salauksessa
- etäkäytössä ja etätöiden sovelluksissa
- sähköisessä allekirjoituksessa.

Tärkeitä tekijöitä salauksen luotettavuudessa ovat itse menetelmän turvallisuustaso, käytön hallinta, jatkuva valvonta ja erityisesti turvallinen avainten hallinta. Salausmenetelmän luotettavuus on varmistettava sitä valittaessa. Menetelmän luotettavuus on parhaiten arvioitavissa, jos se on sertifioitu tuote tai tuote, jonka lähdekoodi on saatavissa menetelmän luotettavuuden arvioitukseksi. Tietoturvallisuusvaatimusten perusteella organisaation tulee itse määrittellä salausohjeensa.

Salauksen käyttöä voidaan laajentaa kaikkeen tiedonkäsittelyyn, kun salaukseen perustuvat tietoturvallisuusohjelmistot integroituvat käytettäviin sovelluksiin ja tulevat käyttäjille läpinäkyviksi (Salauskäytäntöjä koskeva

valtionhallinnon tietoturvallisuussuositus VAHTI 3/2001). Siirrettäessä tietoja avoimissa verkoissa salaus on luottamuksellisuuden suojaamiseksi välttämätöntä.

Poikkeusoloissa salauksen tarpeet korostuvat tiedon aitouden ja käyttövaltuuksien varmistamisessa. Salauksen murtoyritysten vuoksi salausjärjestelmiä on jatkuvasti ylläpidettävä salasana- ja menetelmävaihdoin.

Suojautuminen tietojärjestelmiin kohdistuvilta hyökkäyksiltä

Verkottunut maailmanlaajuinen tietojenkäsittely mahdollistaa suunnitelmalliset hyökkäykset verkkoon, sen tietoihin, tietojärjestelmiin ja tietovarastoihin. Hyökkäyksillä voidaan katkoa tiedon valtaväylät, tuhota tietokantoja, estää organisaatioiden väliset yhteydet tai vaurioittaa verkkoa käyttäviä palveluja ja tuotantotoimintaa sekä paikallisella että kansainvälisellä tasolla. Toimintaa kutsutaan tietosodankäynniksi. Sitä valmistellaan ja käydään jatkuvasti. Osa hyökkäyksistä näkyy vasta myöhemmin hyökkääjän haluamalla hetkellä.

Hyökkäyksen kohteena ovat ensisijaisesti hallinnon, teollisuuden, rahaliikenteen, energiahuollon, liikenteen ja tiedonsiirron keskittymät. Hyökkäysten seurauksena voivat olla mm. oman tiedonsaannin häiriöt ja keskeytyminen, logistiikkapalvelujen estyminen, käytettävyyden häiriöt ja tietojen eheyden särkyminen sekä epäluottamus tiedon ja sen välittäjän oikeellisuuteen.

Informaatiosodalta ja muulta vastaavanlaiselta toiminnalta on välttämätöntä suojautua valtakunnallisesti tärkeiden hallinnon, palvelujen ja tuotannon organisaatioiden tietojenkäsittelyssä. Turvallisuustoimia ovat mm. salaus, suojautuminen tietojärjestelmien murroilta ja virus- ja haittaohjelmilla tapahtuvilta hyökkäyksiltä sekä tiedon oikeellisuuden varmistaminen väärän informaation vaikutusten välttämiseksi. Tärkeiden tietojärjestelmien suojaaminen hyökkäyksiltä edellyttää korkeatasoisia tietoturvaluustoimenpiteitä sekä tehokasta valvontaa tunkeutumisen havaitsemisjärjestelmiä (IDS, Intrusion Detection System) käyttäen.

4.5 Tuotantojärjestelmät, palvelujärjestelmät, jatkuvat verkkopalvelut

Arvioitaessa palvelukykyä ja palvelutason turvaamista on tarkasteltava myös suomalaisten organisaatioiden laajaa ja kasvavaa Internet-riippuvuutta. Verkkojen toimintaan vaikuttaa verkkojen operoinnin hajautuminen useille toistensa verkkoja käyttäville operaattoreille, joiden turvallisuustoimenpiteistä ja varautumisesta käyttäjällä ei ole tietoa. Erityisiä ongelmia palveluiden tuottamiselle saattavat aiheuttaa vaikeudet pitkien palvelu- ja logistiikkaketjujen ja toiminnanohjausjärjestelmien hallinnassa. Toiminnassa se näkyy toimitusketjujen särkyemisestä johtuvina eheyden ja käytettävyyden menetyksinä.

Erityisesti on kiinnitettävä huomiota yrityksen eri puolilla maailmaa sijaitsevien toimipaikkojen Internet-yhteyksien turvaamiseen ja varmistamiseen katkojen varalta. Yhteyksien ylläpito ja toiminnan vaatimien tietojen välittäminen on vaikeaa poikkeusoloissa. Koska yhteyksien käyttö tavallisesti on vaivatonta, siihen ei kiinnitetä riittävästi huomiota eikä varauduta riippuvuudesta seuraaviin vakaviin riskeihin.

4.6 Haavoittuvuuden arviointi

Turvallisuusanalyysi käsittää uhkien ja haavoittuvuuden arvioinnin. Samassa yhteydessä tulee selvittää myös muut toimintaan kohdistuvat tietoturvasuoritusvaatimukset.

Uhkien arvioinnin tarkoituksena on selvittää, millaisia uhkia toimintaan kohdistuu ja millaisiksi riskeiksi ne voivat muodostua. Arvioinnissa pyritään myös selvittämään riskin todennäköisyys ja aiheutuvan vahingon suuruus. Haavoittuvuusanalyysin tarkoituksena on arvioida niitä heikkouksia ja puutteita, jotka tekevät toiminnan alttiiksi erilaisille uhkille.

Uhkatekijöiden tunnistaminen ja niistä organisaation toimintaan, tuotantoon, palveluihin ja tietojenkäsittelyyn kohdistuvien riskien arviointi ovat perustana kaikille tietoturvasuoritus- ja varautumistoimenpiteille. Tavannaisten tietoriskien ohella on arvioitava luonnonkatastrofit, informaatio-sodankäynti, teknologiset riskit ja terrorismi. Avaintekijöitä käytettäväksi uhkien ja haavoittuvuuden arvioinnissa on koottu liitteeseen 4b, tietojenkäsittelyn uhkatekijöitä ja liitteeseen 4c, haavoittuvuuden arviointi.

Tietojenkäsittelyn haavoittuvuuden arviointi kohdistetaan tietoturvasuorituksen, toipumisvalmiuteen ja ainakin tärkeysluokitelluissa yrityksissä myös poikkeusolojen valmiuteen. Haavoittuvuuden arviointi perustuu järjestelmän tuntijoiden - käyttäjien, omistajien, tietoteknisen henkilöstön ja tarkastushenkilöstön - asiantuntemuksen hyväksikäyttöön tietoturvasuorituksen asiantuntijan johdolla. Uudelleenarviointi suoritetaan tietotekniikan tai käyttöympäristön muuttuessa. Arvioinnit eivät tuota tarvittavia tietoja valmiuden luomiseksi, elleivät johto ja esimiehet toiminnan tuntemuksella, riskitietoisuudella ja kokemuksellaan osallistu turvallisuuden kehittämissuoritusprosessiin.

Esiin tulleiden ongelmien seurauksia arvioitaessa on kiinnitettävä huomiota seuraaviin ajankohtaisiin ongelmiin:

- miten paikallisten tietoliikenneyhteyksien menetys vaikuttaa omaan toimintaan
- miten kotimaisten verkkoyhteyksien keskeytys vaikuttaa omaan toimintaan
- miten kansainväliset tietoliikenneyhteydet vaikuttavat omaa toimintaan
- miten kansainvälisten tietoliikenneyhteyksien, huollon, varaosien saannin sekä logistiikka- ja palveluketjujen keskeytys vaikuttavat omaan toimintaan.

Johdon tulee saada tiedot arvioinnin keskeisistä tuloksista kuten

- elintärkeiden toimintojen turvaamisesta
- häiriöiden seurauksista sekä vahinkojen suuruudesta ja vaikutuksista erilaisissa tilanteissa
- turvallisuuden ja valmiuden tasosta ja siinä havaituista puutteista
- toimenpiteistä turvallisuuden ja valmiuden parantamiseksi.

Vahinkojen vaikutusten tunnistamiseksi on tärkeää kehittää valvontaa - seuranta ja raportointia - sekä koota tiedot tietojärjestelmissä sattuvista häiriöistä.

5. VALMIUDEN TAVOITTEET

5.1 Perusturvallisuuden tavoitteet

Perusturvallisuuteen sisältyvät tietoturvallisuus ja toipumisvalmius.

Tietoturvallisuuden tavoitteet

Tietoturvallisuuden tavoitteina ovat korkea tietoaineiston turvallisuus ja tietotekninen turvallisuus.

Tietoturvallisuuteen kuuluu

- tietoturvallisuuden hallinta
- liiketoiminnan tietoteknisten resurssien varmistaminen
- tietoliikenteen turvallisuus
- tietojärjestelmien fyysinen suojaaminen.

Tietoturvallisuuden tavoitteiksi voidaan asettaa seuraavat tekijät:

- tietoturvallisuus perustuu johdon vahvistamaan politiikkaan tai periaatteisiin
- järjestelmissä käsiteltävät tiedot on luokiteltu eheys-, luottamuksellisuus- ja käytettävyyksivaatimusten mukaan
- tietojärjestelmiin, verkkoihin, tiedostoihin ja palveluihin pääsevät vain valtuudet omaavat henkilöt, pääsy on valvottu ja luvaton tunkeutuminen estetty
- järjestelmähallintaan on menettelyt
- tietojenkäsittelytiloihin ja -laitteille eivät ulkopuoliset pääse ja laitteistot on suojattu fyysisiltä vahingoilta
- tiedonsiirto on suojattu siten, etteivät yhteydet ole fyysisten vahinkojen, tunkeutumisen tai tiedon paljastumisen kohteena
- varmuus- ja suojakopioinnilla on varmistettu tietojen jatkuva saatavuus
- avainhenkilöiden työhönotolle ja sijaisuuksien järjestelylle on luotettavat menettelyt
- henkilöstö on koulutettu tehtävien vaatimusten mukaan ja tehtäviinsä motivoitu
- ulkoistettujen palvelujen turvallisuudelle on asetettu vaatimukset ja niiden toteutumista valvotaan
- turvallisuus on sisällytetty laite- ja ohjelmistohankinnan periaatteisiin
- kattavaan käytönvalvontaan on olemassa seuranta ja raportointi.

Turvallisuuden toteutumiselle tärkeää on

- johdon päätökset turvallisuuden suuntaviivoista ja vaatimuksista
- ylimmän ja yksiköiden johdon asettamat toimintojen ja tietojärjestelmien palvelutasovaatimukset
- tulosvastuullisten esimiesten vastuu toimintojensa turvallisuudesta
- yksityiskohtaisiin turvallisuussuunnitelmiin perustuvat toimenpiteet
- henkilökunnan perehdyttäminen
- turvallisuuden kehittäminen osana järjestelmäkehitystä.

Toipumisvalmiuden tavoitteet

Toipumisvalmiuden tavoitteina ovat:

- varautuminen keskeytyksiin ja tietotekniisiin erityistilanteisiin, jotka rajoittavat tietotekniikan käyttöä tai muulla tavoin vakavasti vaarantavat toiminnan ja tietoturvallisuuden tai estävät tietotekniikan käytön
- varajärjestelmien suunnitelmallinen käynnistäminen
- tietojärjestelmän ja tiedonsiirron keskeytymisestä syntyvien vahinkojen rajaaminen siten, ettei keskeytys vaaranna toimintaa
- nopea palautuminen toimintaa rajoittavista varajärjestelmistä takaisin normaalituotantoon ennen toiminnan jatkuvuuden vaarantumista.

Toipumisvalmiudella luodaan perusta myös poikkeusolojen valmiudelle.

5.2 Poikkeusolojen valmiuden tavoitteet

Poikkeusolojen valmiuden tavoitteina ovat

- oman toiminnan turvaaminen poikkeusolojen vaikutuksista huolimatta
- valtiovallan asettamien poikkeusolojen valmiusvaatimusten täyttäminen
- välttämättömän tietojenkäsittelyn ylläpito resurssien vähentyessä jyrkästi
- varautuminen tietojenkäsittelyn korvaaviin järjestelmiin
- edellytysten luominen elpymiselle ja
- palaaminen normaaliin toimintaan.

Poikkeusolojen valmiuden kehyksinä ovat

- poikkeusolojen tuotantotoiminnan tason määrittely
- poikkeusolojen tietohallinnon määrittely poikkeusolojen tuotantotason ja oman toiminnan turvaamiseksi
- tietojenkäsittelyn sopeuttaminen vähentyneiden resurssien mahdollistamalle tasolle
- erityistilanteisiin luotu valmius ja sen suuntaaminen poikkeusolojen toimintojen säilyttämiseen
- valtiovallan säännöstelyllä ja ohjauksella asetetut toiminnan puitteet
- erityisesti ulkomaisten tietojenkäsittelylaitteistojen, tiedonsiirtoyhteysien ja tukipalvelujen puutteet
- Internet-yhteysien puuttuminen
- varautuminen toimimaan muualla ja luopumaan tietotekniikan käytöstä
- tietojenkäsittelyn perusedellytysten varmistaminen suojakopioin kriisistä elpymiseksi.

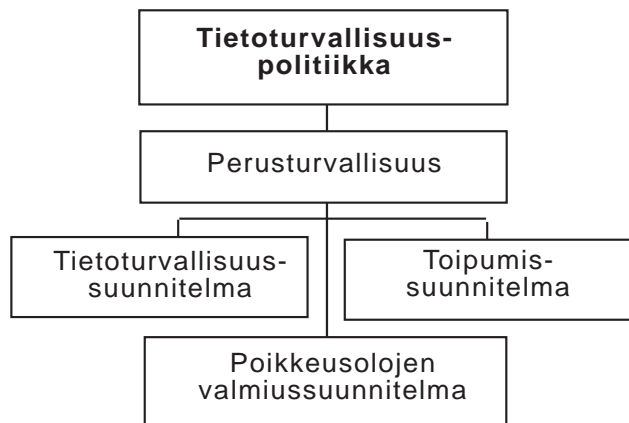
6. TIETOJENKÄSITTELYN PERUSTURVALLISUUS

6.1 Tietoturvallisuuden ja toiminnan jatkuvuuden varmistamisen perusteet

Ellei organisaatiolla ole selkeästi määriteltyä tietoturvallisuuspolitiikkaa ja toimintastrategioihin perustuvia tietoturvallisuuslinjauksia, johdon on välttämätöntä tarkistaa toimintatavat ja vahvistaa periaatteet. Tarkistuksen yhteydessä on huomattava, etteivät tietoteknisen henkilöstön laajataan tietotekniikkälähtöisesti toteuttamat turvallisuustoimenpiteet välttämättä tue nopeasti muuttuvia palvelujen ja tuotannon tarpeita.

Perusturvallisuudessa varaudutaan tietoturvallisuussuunnitelmin vahingoista, virheistä, häiriöistä sekä sisäisistä ja ulkoisista luvattomuuksista aiheutuvien riskien torjuntaan sekä toipumissuunnitelmin vakaviin keskeytyksiin. Nämä suunnitelmat ovat tarpeellisia kaikissa tietotekniikkariippuvissa organisaatioissa.

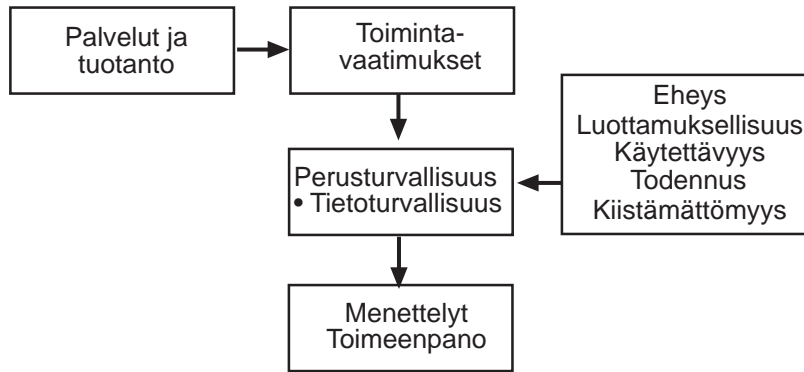
Tietojenkäsittelyn turvallisuus ja toiminnan varmistaminen



Tärkeysluokitelluilta yrityksiltä edellytetään lisäksi tietojenkäsittelyn valmiussuunnitelmaa poikkeusoloihin. Muidenkin yritysten on aiheellista selvittää valmiustarpeet, vaikka eivät olisikaan velvoitettuja laatimaan valmiussuunnitelmia.

6.2 Tietoturvaluissuunnitelma

Tietoturvaluisuuden reunaehtoina on normaaliolojen palvelujen ja tuotannon tason ja laadun ylläpito sekä toisaalta eheys-, luottamuksellisuus-, käytettävyys-, todennus- ja kiistämättömyysvaatimukset. Nämä tekijät sanelevat toimintavaatimukset tietoturvaluisuudelle.



Tietoturvaluisuuden arviointi

Uhkien ja haavoittuvuuden ohella tietoturvaluissuunnittelun yhteydessä arvioidaan tietoturvaluisuuden taso. Tietoturvaluisuuden arvioinnissa tarkasteltavia seikkoja on koottu liitteeseen 4c haavoittuvuuden arviointi, kohtaan tietoturvaluisuuden arviointi.

Tietoturvaluisuuden suunnittelu

Tietoturvaluissuunnitelmaan sisällytetään kaikki toimenpiteet, joita tarvitaan tavanomaisen toiminnan ja sen tietoturvaluisuuden ylläpitämiseksi hyvän tiedonhallintatavan mukaan.

Tietoturvaluissuunnittelussa käsitellään hallinnollisen turvaluisuuden, henkilöstöturvaluisuuden, tietoaineistoturvaluisuuden, laitteistoturvaluisuuden, ohjelmistoturvaluisuuden, tietoliikenneturvaluisuuden, käyttöturvaluisuuden ja fyysisen turvaluisuuden vaatimukset ja toimenpiteet.

Tietoturvaluissuunnitelma on useimmiten toimiala- tai yksikkökohtainen.

Tietoturvaluissuunnitelman jäsentelystä on esitetty esimerkki liitteessä 5 tietoturvaluisuuden suunnittelu, kohdassa tietoturvaluissuunnitelma.

Hallinnollinen tietoturvaluisuus - johtaminen

Hallinnollinen tietoturvaluisuus on tietoturvaluisuuden johtamistoiminto. Se sisältää ne periaatteet, määrittelyt ja järjestelyt, joilla johto ohjaa koko tietojenkäsittelyn turvaluutta. Toimenpiteiden toteutus kuuluu ensi sijassa yksiköiden johdolle. Tietoturvaluisuuden linjaukset liittyvät usein tietohallintostrategiaan, johon tietoturvaluisuuden tulee liittyä myös muutoksia ja kehittämistä ajatellen.

Henkilöstön koulutusjärjestelyt sekä ohjeistus-, valvonta- ja tarkastusmenettelyt ovat välttämättömiä toimenpiteiden käynnistämiseksi ja ylläpitämiseksi. Ulkoistaminen vaatii omalta henkilöstöltä tietoturvallisuuden osaamista, jotta palveluyrityksen hoitamat tietotekniikkapalvelut voidaan hoitaa turvallisesti ja valvoa korkeatasoisesti. Suunnitelmissa otetaan huomioon oman tietoteknisen henkilöstön tietoturvallisuuden osaaminen ja sen kehittäminen.

Henkilöstöturvallisuus

Tietojenkäsittely tulee suojata henkilöstön aiheuttamilta luvattomuuksilta ja hyökkäyksiltä. Ulkoisten uhkien ohella tietojen sisäisen väärinkäytön ja haitanteon riskit ovat lisääntyneet. Luotettavuusriskejä aiheuttavat muutokset yhteiskunnassa, kilpailun kiristymisen, erilaisten ristiriitaryhmien toiminta ja huumeiden käyttö sekä tietojenkäsittelyyn osallistuvien henkilöiden suuri määrä organisaation sisällä ja ulkopuolella.

Lyhyiden työsuhteiden epävakaisuuden ja alihankinnan vuoksi yritysten toimintaan osallistuu vaihtuvaa ja usein työympäristössä lähes tuntematonta henkilöstöä. Työntekijöiden motivaatio ja elämäntilanne saattavat muuttua ja johtaa luvattomuuksiin, häirintään ja tietojen luvattomaan luovutukseen. Käyttövaltuuksia annettaessa on entistä tarkemmin kiinnitettävä huomiota henkilöstön luotettavuuteen. Muun muassa palkkauksen ja uudelleensijoittamisen yhteydessä tarkistetaan taustatiedot ja seurataan motivaatiota ja luotettavuutta. Soveltuvuustesteihin voidaan sisällyttää luotettavuutta selvittäviä osuuksia.

Nopea kehitys, osaamisen kapea-alaisuus sekä tietojenjärjestelmien hallinnan keskittyminen yksittäisille asiantuntijoille lisää riippuvuutta avainhenkilöistä. Tietojenkäsittelyn tehokkuuden ja kasvavien vaatimusten aiheuttamat paineet pakottavat kiinnittämään entistä enemmän huomiota avainhenkilöriskeihin. Niihin voidaan vaikuttaa suunnittelemalla ajoissa sijaisjärjestelyt, kouluttamalla varahenkilöt ja dokumentoimalla tietojärjestelmät.

Suunnittelussa käsiteltäviä seikkoja ovat mm.:

- työnhakijan taustatarkistus
- työntekijöiden ja sopimuskumppaneiden salassapitosopimukset
- henkilöstön motiivointi tietoturvallisuuden kannalta, koulutus
- varahenkilöjärjestelyt
- ostopalveluiden henkilöstöturvallisuuden hallinta
- huumeetestausta, kun se on mahdollista
- puuttuminen turvallisuusriskejä aiheuttavaan toimintaan.

Henkilöriskien hallinta on henkilöstöhallinnon osatehtävä. Henkilöturvallisuuden vastuu on ensisijaisesti hallinnollisilla esimiehillä.

Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan tiedon salassapitoa, tiedon ja tietoaineiston käytettävyyttä, tiedon turvallista käsittelyä ja säilytystä sekä lopulta tarkoituksenmukaista tietojätteen hävittämistä.

Tietojärjestelmistä saatavien tietojen on oltava oikeaa, ajankohtaista ja täydellistä sekä muodoltaan sellaista, että sitä voidaan välittömästi käyttää haluttuun tarkoitukseen. Tietosisällön heikkouden seurauksia ovat mm.

virheellisen tiedon leviäminen jatkokäsittelyyn, päätösten tekeminen virheellisin tiedoin, työmäärän lisääntyminen ja huono yrityskuva. Tiedon tulee olla ehjää niin, ettei se muuttuneena, vajavaisena tai väärin ymmärrettyinä johda virheelliseen tulokseen, päätöksentekoon tai toimintaan ja siten synnytä vahinkoja levitessään. Luvattoman käytön riskit edellyttävät laajoissa tietojärjestelmissä yhä perusteellisempaa tietojen suojaamista sekä oikeellisuuden ja käytettävyyden varmistamista.

Viranomaisten ja yritysten tietojärjestelmissä voi olla tietoja, jotka säädösten perusteella tai muista syistä on suojattava.^{12, 13}

Tallennetun tiedon ja ohjelmistojen suojaaminen vahingoilta, vahingoittamiselta ja menetyksiltä koskee kaikkia tietojärjestelmien omistajia. Tiedon, tietokantojen ja verkoissa siirrettävien tietojen suojaaminen edellyttää salausmenetelmien käyttöä.

Tiedon suojaamisen perustana on tietojen, tietojärjestelmien ja sovellusten luokitus luottamuksellisuuden mukaan ja sen perusteella käyttöön otetut suojausmenetelmät.¹⁴

Tietoaineiston turvallisuus ei kohdistu vain tietojärjestelmiin. Luokituksen perusteella määritellään käsittelysäännöt myös manuaaliselle tiedonkäsittelylle.

Tiedot ja ohjelmistot on tietojärjestelmissä, lähiverkoissa ja tiedonsiirrossa suojattava käytettävyyden ja oikeellisuuden varmistamiseksi luvattomalta käytöltä, muuttamiselta ja tuhoamiselta. Aineistoa ei toisaalta saa säilyttää liian kauan käytössä, vaan palvelimilta tulee poistaa turhat tiedot.

Tietosuoja

Tietosuoja on tietoaineiston turvaamisen erikoisalue. Sillä tarkoitetaan henkilörekisterien tietoturvallisuutta. Arkaluonteisten henkilötietojen käsittely on kielletty laissa määriteltyjä poikkeuksia lukuun ottamatta.¹⁵ Henkilörekisterin pitäjänä yrityksen on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomilta ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Tarpeeton henkilörekisteri on hävitettävä.

Itsenäisen, rekisterinpitäjän lukuun toimivan elinkeinonharjoittajan on ennen tietojen käsittelyyn ryhtymistä annettava rekisterinpitäjälle asianmukaiset sitoumukset ja muutoin riittävät takeet henkilötietojen suojaamisesta edellä tarkoitetulla tavalla.

Teleyrityksen tulee huolehtia teletoimintansa tietoturvasta yksityisyyden ja oikeutettujen etujen suojaamiseksi.^{16, 17} Teleyrityksen tulee varmistaa teletoimintansa tietoturva myös poikkeusoloissa osallistumalla valmiussuunnitteluun, valmistelemalla etukäteen poikkeusoloissa tapahtuvaa toimintaa sekä muin toimenpitein.

Tiedon luokitus

Tietojen luokitus on keskeinen tietoaineiston turvaamisen perusta. Siinä ilmoitetaan salassapitovaatimus. Luokituksen tarkoituksena on jakaa tiedot ryhmiin, joille asetetaan käsittelysäännöt. Niiden tulee sisältää ohjeet tuloasteilla, tietovälineillä ja muisteissa olevan tiedon käsittelystä, säilytyk-

sestä, tuhoamisesta ja viestittämisestä erilaisia tiedonsiirtoyhteyksiä käyttäen. Tiedot ja tietoaineisto on arvioitava ja luokiteltava sisällön ja sen perusteella, miten haavoittuvia ne ovat asiattomalle käsittelylle ja siitä aiheutuville menetyksille ja paljastumisen seurauksille. Luokituksen perusteella toteutetaan tietojen suojaaminen käyttäen ohjelmistojen turvallisuusominaisuuksia tietoihin pääsyn, luottamuksellisuuden, oikeellisuuden, eheyden, käytettävyyden, todentamisen ja kiistämättömyyden valvonnassa.

Laiassa viranomaisen toiminnan julkisuudesta on määritelty viranomaisen toiminnassa ne alueet, joilla luokittelu on tehtävä. Käsiteltäessä ja säilytettäessä säädösten ja ohjeiden perusteella salassa pidettäviä, yksityisyyden suojan tai muun syyn vuoksi suojattavia tietoja on salassapito varmistettava käsittelyn kaikissa vaiheissa.

Viranomaisen tiedot tai tietoaineisto on ^{12, 13}

- Julkinen, ellei sitä lain viranomaisen toiminnan julkisuudesta tai muun säädöksen perusteella ole määritelty salassa pidettäväksi tai muu kuin lainsäädännön säätämä tieto silloin, kun sen paljastumisesta ei ole haitallisia seurauksia
- Luottamuksellinen (3. turvaluokka), kun sen paljastuminen asiattomille ja väärinkäyttö aiheuttaa haitallisia seurauksia
- Salainen (2. turvaluokka), kun se lainsäädännön perusteella on määritelty salassa pidettäväksi tai sen paljastuminen asiattomille ja väärinkäyttö aiheuttaa huomattavia haitallisia seurauksia
- Erittäin salainen (1. turvaluokka), kun se lainsäädännön perusteella on määritelty salassa pidettäväksi tai sen paljastuminen asiattomille ja väärinkäyttö aiheuttaa erittäin haitallisia seurauksia.

Yrityksissä luokittelun perustana on sen oma tiedon ja tietoaineistojen salassapitotarve. Salassa pidettäviä aineistoja ovat esimerkiksi strategiset suunnitelmat, yrityssuunnitelmat, laajakantoiset kehittämissuunnitelmat, tuotekehitys, reseptiikka ja tarjoustiedot. Aineiston luokitukseen ja merkintöihin voidaan käyttää soveltaen valtionhallinnon ohjeita (liite 3). Yritystä paremmin palvelevaa muunlaista luokitusta voidaan myös käyttää.

Tiedon suojaaminen koskee tietoa kaikissa muodoissaan eli puhuttuna, saneltuna, kirjallisena, kuvina, piirroksina ja datana. Tietojärjestelmässä käyttövaltuuksien on vastattava salassapitoluokkaa, tulosteet ja tallenteet on käsiteltävä luokituksen mukaisesti ja tiedonsiirrossa tiedon suojauksen on oltava luokituksen tasoinen.

Aineiston salassapitotarve on määriteltävä ja siitä seuraava luokittelu päätettävä aineistoa luotaessa. Luokitus toteutuu aineiston käsittelyssä, järjestelmien, sovellusten ja tietojen käyttövaltuuksien jakelussa, pääsynvalvonnassa sekä salauksessa. Käyttövaltuudet myöntää toiminnasta vastaava johto tai tietojärjestelmän omistaja, vaikka ne käytännössä asettaa tietojärjestelmän pääkäyttäjä tai tietotekninen henkilöstö. Erittäin salainen –luokassa pääsynvalvonnan ja muun tiedon suojauksen on oltava korkeinta tasoa, jos tietoa edes käsitellään tietojärjestelmässä.

Tietojärjestelmissä luottamukselliset ja salaiset aineistot sijoitetaan omiin suojattuihin hakemistoihinsa. Valtionhallinnon ohjeiden mukaan erittäin

salainen aineisto käsitellään erillisellä turvamikrolla, eikä sitä saa lähettää sähköisissä tietojärjestelmissä. Salainen ja luottamuksellinen aineisto voidaan lähettää sähköisissä tietojärjestelmissä ainoastaan riittävän vahvasti salattuna. Nämä käytännöt sopivat noudatettavaksi myös yrityksissä.

Suunnittelussa käsiteltäviä seikkoja ovat mm.:

- tietojen luokitus ja luokitusperiaatteet
- manuaaliset ja tietotekniset käsittelysäännöt
- erityisesti erittäin salaisen ja salaisen aineiston suojaaminen
- henkilörekisterien käsittely ja suojaaminen
- ohjeistus
- koulutus.

Tietotekninen turvallisuus

Laitteistoturvallisuus

Laitteistoturvallisuudella pyritään ensisijaisesti vähentämään laitteista aiheutuvia häiriöitä ja keskeytyksiä. Prosessointikyvyn paranemisen vuoksi tietotekniset laitteet ja ohjelmistot uusiutuvat nopeasti, mikä vaikeuttaa käyttöönottoa, ylläpitoa ja yhteensopivuutta. Tehokkuuden ja suuren tallennuskäytön hyödyntäminen aikaansaa keskittyneitä, riskialttiita laitteita tietojärjestelmien ja tietovarastojen. Laitteistojen valinnalla on suuri vaikutus turvallisuuteen. Esimerkiksi testattujen, korkeatasoisten levyjen käyttö tietovarastoina on suositeltavaa.

Suunnittelussa käsiteltäviä seikkoja ovat mm.:

- yhteensopivuuden varmistaminen
- laitteistojen häiriötön toiminta ja käytettävyys
- laitteiden vikasietoisuuden huomioon ottaminen hankinnoissa
- laitteiden, varaosien ja tarvikkeiden saatavuus ja korvattavuus
- ylläpito
- tehokkuuden lisääntymisestä aiheutuva monien yksittäisten laitteiden ja työympäristöjen turvallisuustarpeiden kasvu
- tehokkuuden hyödyntäminen järjestelmien turvallisuuden valvonnassa ja sen automatisoinnissa.

Varastojen keskittyminen ulkomaille harvoin pisteisiin saattaa viivyttää hankintoja varalaiteratkaisujen perustuessa ulkomaisiin toimituksiin. Laitteiden ja varaosien ulkomainen saatavuus on pääasiassa poikkeusolojen ongelma. Keskuslaitteiden suuri määrä verkottuneessa toiminnassa antaa mahdollisuuksia organisaatioiden sisäisiin varalaittejärjestelyihin.

Ohjelmistoturvallisuus

Ohjelmistoturvallisuuden tarkoituksena on suunnata hankinnat sellaisiin ohjelmistoihin, jotka omilla piirteillään tukevat turvallisuutta. Ohjelmistoturvallisuuteen kuuluvat myös varsinaisten turvallisuusohjelmien luotettavuus ja laadun varmistus. Tietojärjestelmissä tulee olla kattavat järjestelmähallinnan, pääsynvalvonnan, tiedon suojauksen ja käytönvalvonnan menetelmät. Laajankin järjestelmän turvallisuus voi pysyvästi vaarantua, ellei ohjelmistohankintojen yhteydessä varmisteta ohjelmistojen turvallisuusominaisuuksia tai jos niitä ei ole otettu käyttöön tietojärjestelmien omistajien vaatimusten mukaan. Uusia sovelluksia ei saa hyväksyä tuotantokäyttöön ennen testausta, tarkastamista ja hyväksymistä. Tietojärjes-

telmien hajauttamisen ongelmana on vaikea versiohallinta avoimessa ympäristössä. Versioerot voivat synnyttää toimimattomia yhdistelmiä.

Suunnittelussa käsiteltäviä seikkoja ovat:

- tietojärjestelmäkehityksessä ja -hankinnoissa noudatettavat tietoturvallisuusmenetelmät
- tietojärjestelmäkokonaisuuksien suojausarkkitehtuurin luominen
- ohjelmistojen turvallisuuspiirteiden yhteensopivuus ja turvallisuustaso
- ohjelmistojen turvallisuuden ylläpito ja päivitettävyys
- kattava virustorjunta
- pääsynvalvonta-, tunnistus-, salaus- ja varmistamismenetelmät
- tapahtumakirjaukset ja poikkeavien tapahtumien erottelu
- tietoturvallisuusrikkomuksien havainnointimenetelmät
- toimenpiteet ohjelmistoturvallisuuden ja laadun ylläpitämiseksi ja kehittämiseksi
- testaus ja tuotantoon hyväksyminen.

Tietoturvallisuuden kannalta käyttövaltuuksien hallinta on eräs tärkeimmistä turvallisuusmenettelyistä. Sen tulee noudattaa tiukasti työtehtävissä sallittavia valtuuksia.

Ohjelmistojen tulee sisältää tapahtumakirjaukset (loki) sekä tapahtumien luokittelun ja raportoinnin, joihin pääsyn- ja käytönvalvonnan järjestelyt voidaan perustaa. Tapahtumakirjausten seurannan ja raportoinnin puutteiden vuoksi vaarannetaan koko tietojenkäsittelyn turvallisuus.

Käyttöjärjestelmien ja ohjelmistojen pysyvät puutteet altistavat tietotekniikan viruksille ja muille haittaohjelmille. Virukset voivat aiheuttaa vakavia keskeytyksiä ja äärimmillään koko toiminnan lamautumisen. Niiden vuoksi on varauduttava mm. laajan, jopa globaalin sähköpostijärjestelmän sulkemiseen viruksen leviämisen estämiseksi. Viruksilta suojautumiseksi on verkoissa, tietojärjestelmissä ja työasemilla järjestettävä kattava virus- ja haittaohjelmien torjunta ja ohjelmien päivitykset sekä varmistettava tietoteknisen henkilöstön riittävä osaaminen virustorjunnassa. Virusten torjunta ei voi jäädä yksittäisten käyttäjien ja kieltojen varaan. Viruksilta suojautumiseen kuuluu myös hyvin hoidettu puhtaiden varmuus- ja suojakopioiden ylläpito sekä tarpeettoman sähköpostiaineiston poistaminen. Haittaohjelmat voivat aiheuttaa nykyisiä virusvahinkoja huomattavasti vakavampia ongelmia.

Tietoliikenneturvallisuus

Tietoliikenneturvallisuuden tarkoituksena on tietoverkon, tietoliikenteen ja siirrettävän tiedon suojaaminen sekä verkon keskeytysten hallinta ja yhteyksien varmistaminen.

Verkkopalveluissa ei enää voida erottaa tietojenkäsittelyn ja tiedonsiirron turvallisuutta toisistaan vaan turvallisuutta ja sen varmistamista on tarkasteltava kokonaisuutena. Laajoissa tietoverkoissa turvallisuustoimenpiteet hajautuvat monille tahoille, joihin järjestelmän omistajan on vaikea vaikuttaa. Suojaamattomat verkot ovat alttiita yhteyksien väärinkäytölle, tietojärjestelmiin tunkeutumiselle ja sähköpostin tai muun siirrettävän tiedon anastukselle ja muuttamiselle. Verkoissa tietoturvallisuus edellyttää siten sekä tietojenkäsittelyn korkeatasoista suojaamista että tietoliikenteen suojaamista.¹⁸

Suunnittelussa käsiteltäviä seikkoja ovat:

- riippuvuus tietoliikenteestä sekä alttius häiriöille ja tahallisille yhteyksien häirinnälle
- verkkoliittymien turvallisuuden periaatteet
- verkon hallinnan ja turvallisuuden hallinnan järjestelyt
- Internet-, intranet- ja ekstranet-verkkojen turvallisuus
- palomuurien tarpeet ulkoisten verkkojen liittymäkohdissa
- sisäisten salaisten verkkojen ja kriittisten tietojärjestelmien erottaminen ulkoisista ja muista sisäisistä verkoista kokonaan tai palomuuria käyttäen
- tapahtumien havainnointimenettelyt
- toimenpiteet tunkeutumisyrityksissä ja tietoturvasuoritusrikkomuksissa
- oikeudettomien yhteydenottoyritysten katkaisu
- vahva tunnistus ja varmenteiden käyttö
- tiedon suojaaminen salauksella
- turvallisuudeltaan tunnettujen yhteyksien käyttö, kiinteät ja kytkentäiset verkot
- yhteyksien varmistaminen ja varayhteydet
- verkon tietoturvasuorituksen valvonnan yleiset järjestelyt.

Internet-verkkopalvelut käyttävät turvallisuudeltaan heikkoja yhteyksiä. Internet-yhteydet edellyttävät, että oma verkko (intranet, ekstranet) eristetään reitittimillä ja yhdyskäytävillä palomuuria käyttäen. Julkisia tietoja omasta verkosta Internetiin tarjoavat palvelinlaitteet erotetaan organisaation sisäisestä verkosta sekä tuotantoverkko edelleen sisäisestä verkosta. Päätösten julkiseen verkkoon liittymisestä tulee perustua johdon harkintaan liittymätarpeesta ja suhteutettuna syntyviin riskeihin. Internet-verkon ehdoilla toimittaessa voidaan verkkoon toimittaa vain julkista aineistoa. Internetin tavoin on tarpeellista erottaa alihankkija- ja palveluyritysyhteydet omista verkoista palomuurilla. Ilman luotettavien salausmenetelmien käyttöä ei tietoa voida suojata verkoissa ja tietoliikenteessä.

Luvattomaan tietojenhankintaan kansainvälisistä tietoliikenneverkkoista on aiheellista kiinnittää huomiota. Internetistä ja kansainvälisiltä linkki- ja satelliittiyhteyksiltä tietoja siepataan järjestelmällisesti ja suunnitelmallisesti salaamattomien viestien tietosisällön perusteella hakien.

Lähiverkkoihin kytkeytyminen on teknisesti yksinkertaista ja vaikeasti havaittavaa. Myös lähiverkkojen fyysisestä turvallisuudesta on huolehdittava.

Käyttöturvallisuus

Käyttöturvallisuuden tarkoituksena on huolehtia tietojärjestelmien luotettavasta toiminnasta. Käyttöturvallisuus koskee yksittäisiä palvelimia, keskuslaitteita, tietoliikenneyhteyksiä, verkkoja ja näiden valvontaa.

Suunnittelussa käsiteltäviä seikkoja ovat:

- tietotekniikan turvallisen käytön vaatimien olosuhteiden ylläpito
- toimivuuden valvonta ja häiriöraportointi
- käyttövaltuuksien valvonta
- tietoturvasuorituksen loukkausten havainnointi
- ohjelmistojen ylläpidon turvallisuustoimenpiteet sekä
- varmuus- ja suojakopiointi.

Käytön turvallisuustarpeita korostaa monimuotoinen, vaikeasti hallittava tekninen, toiminnallinen, yksittäisten osajärjestelmien toimivuudesta riippuva kokonaisuus. Lisäksi käytön järjestelyihin vaikuttavat ylläpito-, huolto- ja tukipalvelujen hajautuminen monille tahoille, palvelujen ulkoistaminen, suuri käyttäjäkunta ja verkkojen ja työasemien runsaslukuisuus, valvottavien liittymien suuri määrä sekä laajan teknisen järjestelmän monet häiriötekijät monissa pisteissä.

Käyttöturvallisuus on koko organisaation kattava toiminto. Verkon solmukohdissa ja keskuslaitteilla käytön turvallisuuden ylläpito ja valvonta on tietoteknisen henkilöstön vastuulla ja sitä tulee ohjata myös sovellusten omistajille. Valvonnan painoituksissa on otettava huomioon tietojärjestelmän osien erilainen merkitys - toisten osajärjestelmien merkitys on vähäinen ja toisten jopa kriittinen. Käyttöturvallisuus kohdistuu ensisijaisesti kriittisiin järjestelmänosiin.

Käyttöturvallisuuden yhteydessä on huolehdittava tietoaineiston turvallisuudesta, salassapidosta sekä henkilöturvallisuuden varmistamisesta.

Fyysinen turvallisuus

Fyysisen turvallisuuden tarkoituksena on toiminnalle turvallisen ja häiriöttömän käyttöympäristön luominen ja ylläpito. Suojattava käyttöympäristö on laaja, moniin pisteisiin ja toimistojen työasematiiloihin ulottuva kokonaisuus.

Suunnittelussa käsiteltäviä seikkoja ovat:

- tilojen ja laitteiden turvallinen sijoitus
- tietotekniikan käyttöympäristön toimintaolosuhteiden luominen ja ylläpito (konesali-, palvelin-, ristikytkentä-, lähiverkko-, tietoliikennelaite-, varajärjestelmä- ja teletilat sekä näitä ympäröivä suoja-alue)
- ympärysjärjestelmien varmistaminen (sähkönsyöttö, ilmastointi, lämmitys sekä konesali- ja palvelintilojen olosuhdehälytykset)
- tallenteiden, varmuus- ja suojakopioiden säilytystilojen turvallisuus, aineiston paloturvallinen ja tietoturvallinen säilytys
- työasemien, palvelimien ja muiden laitteiden suojaaminen anastuksilta sekä toiminnan sabotoinnilta
- paloturvallisuus, palo-osastointi ja pelastustoiminta
- suojautuminen vesivahingoilta
- kiinteistön ja erikoistilojen valvonta (laite-, tietojenkäsittely- ja teletilat)
- kulunvalvonta ja valvontajärjestelmien käyttö
- suojautuminen säteilyltä
- fyysisen turvallisuuden ylläpito, valvontajärjestelmien ja sammutuslaitteiden tarkastus, testaus ja huolto
- varautuminen onnettomuuksiin ja luonnontuhoihin
- poikkeusolojen valmiuden vaatimukset laiteiloille.

Tietojenkäsittelyn fyysisen turvallisuuden suunnitteluun tarvitaan usein koko kiinteistön kattavaa turvallisuustarpeiden ja -ratkaisujen arviointia. Tietojenkäsittelytilojen fyysisen turvallisuuden parannukset on tarkoituksenmukaista käsitellä aina rakennus- ja korjaushankkeiden yhteydessä. Uudisrakennuksen tietojenkäsittelytilojen suunnittelu on aloitettava jo hankkeen alkuvaiheessa.

Tietojärjestelmien omistajat asettavat osaltaan fyysisen turvallisuuden vaatimukset. Kiinteistön rakenteiden ja turvallisuusjärjestelmien käytännön

toteutuksen ja ylläpidon vastuut on tarkoituksenmukaista sisällyttää kiinteistön vastuuhenkilöiden tehtäviin. Turvallisuusteknisten järjestelmien valvonta on turvallisuushenkilöstön ja kiinteistönhoidon tehtävä.

Suunnittelussa on normaalitoiminnan tarpeiden ohessa nähtävä myös poikkeusolojen kasvavat fyysisen turvallisuuden ja valvonnan tarpeet. Valta-kunnallisesti tärkeät keskuslaitteistot pyritään sijoittamaan väestönsuojatiloja vastaaviin tiloihin siten, että ne on helpommin suojattavissa ja erotettavissa tarpeettomalta henkilöliikenteeltä. Erityisesti tärkeiden poikkeusoloissa käytettävien verkon laitteiden sijoituksessa on otettava huomioon elektromagneettisen pulssin (EMP) vaikutukset ja tärkeiden laitteiden suojaustarve. Tärkeiden tietotekniikkakeskittymien paikallisessa sijoittamisessa ja suojaamisessa on selvitettävä suojautuminen radiotaajuusaseilta (HPM-ase).

Valvonta

Valvonnan ensisijaisena tarkoituksena on tietoturvallisuuden rikkomisyri-tysten havaitseminen ennalta rikosten torjumiseksi sekä turvallisuustoi-menpiteiden toteutumisen ja noudattamisen valvonta. Valvonta palvelee myös tietoturvallisuuden kehittämistä. Tietoturvallisuuden valvonta muodostuu seurannasta ja raportoinnista.

Suunnittelussa käsiteltäviä seikkoja ovat:

- valvonnan yleisjärjestelyt ja vastuut
- tietoturvallisuuden loukkausyritysten havainnointi ja loukkausten käsittely
- IDS (Intrusion Detection System) - verkonvalvonta- ja tunkeutumisen esto-ohjelmien käyttö
- käyttöhenkilöstön, palvelujen toimittajien ja muun henkilöstön aiheuttamien häiriöiden seuranta
- keskus- ja oheislaitteissa sekä tietoliikenneyhteyksissä esiintyneet häiriöt
- järjestelmätuki- ja sovellusohjelmahäiriöt
- sähkönjakelusta, ilmastoinnista tai muista seikoista johtuneet käyttöympäristöhäiriöt
- tietoturvallisuuden seurannan järjestelyt
- raportoinnin järjestelyt.

Tietoturvallisuuden seurannan tulee olla jatkuvaa ja kattavaa. Kaikki tietojenkäsittelyssä tapahtuneet virheet, häiriöt ja tietoturvallisuuden rikkomukset kirjataan, raportoidaan ja selvitetään. Osa virhe- ja häiriötiedoista voidaan kerätä käyttöjärjestelmien ja ohjelmistojen lokitiedoista sekä laitteistojen häiriöilmoituksista. Verkoissa tietoturvallisuusrikosten seuranta järjestetään tapahtumien havainnointiohjelmistoin. Tietojärjestelmien kehittämisessä, käytössä ja ylläpidossa valvotaan valmiudesta ja turvallisuudesta annettujen ohjeiden sekä sovellustyön standardien noudattamista.

Esimiesten tehtävänä on tarkastusten järjestäminen omilla vastualueillaan. Tarkastettavia kohteita ovat esimerkiksi ohjelmien käyttöönotto ja testaus, salasanamenettelyt ja salassapito, tiedostojen salaaminen, käyttövaltuudet, tulosteiden käsittely sekä varmuus- ja suojakopioiden ylläpito ja säilytys. Osaan tarkastuksista voidaan käyttää erityisiä tarkastusohjelmia.

Turvallisuusjohdolle tulee raportoida havaituista tietosuojarikkomuksista. Ylimmän johdon tulee saada raportti turvallisuudesta ainakin kerran vuodessa.

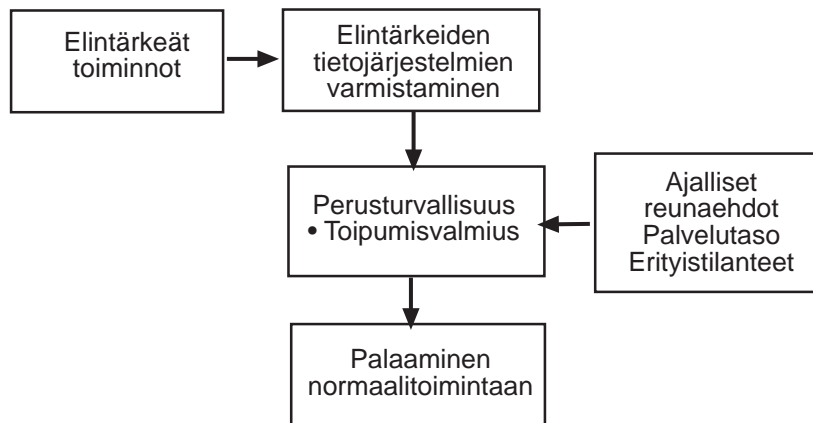
Tietoturvaluissuunnitelma (esimerkki)

Sisältö

- Hallinnolliset turvallisuustoimenpiteet ja johtaminen
 - turvallisuuden tarkoitus ja tavoitteet
 - johdon hyväksymät periaatteet ja linjaukset
 - toteutusidea
 - vastuut, toiminnan organisointi ja johtaminen
 - turvattavat toiminnot ja järjestelmät
 - sopimukset
- Tietoturvaluissuustoimenpiteet ja menettelyt
 - hallinnollinen turvallisuus
 - henkilöstöturvallisuus
 - tietoaineistoturvallisuus, varmuus- ja suojakopiointi
 - tietotekninen turvallisuus
 - laitteistoturvallisuus
 - ohjelmistoturvallisuus
 - tietoliikenneturvallisuus
 - käyttöturvallisuus
 - fyysinen turvallisuus
- Ulkoistettujen tietojenkäsittelytoimintojen turvallisuus
- Tuotannon ja palvelujen varmistaminen
- Tietoturvaluissuustoimenpiteiden toteuttaminen hankintojen yhteydessä
- Tietoturvaluisuuden valvonta, seuranta, tarkastus ja testaus
- Ohjeet
- Valmiudet ja menettelyt vahinkotilanteisiin, varautuminen erityistilanteisiin
- Poikkeusolojen valmius
- Koulutus
- Suunnitelman päivitys ja toimenpiteiden ylläpito
- Raportointi johdolle

6.3 Toipumissuunnitelma

Toipumisvalmiuden reunaehtoina ovat elintärkeiden toimintojen ylläpito vakavissa keskeytystilanteissa sekä toisaalta suurin sallittava keskeytysaika ja toipumisen aikana vaadittava palvelutaso. Nämä tekijät sanelevat toipumissuunnittelun vaatimukset ja varajärjestelmien tarpeet.



Toipumissuunnittelun tärkeimpänä tavoitteena on valmiuden luominen vahinkoihin, joissa voidaan menettää toiminnan kannalta kriittisten tietojärjestelmien tai niiden osien käytettävyys. Yhdessä tietojärjestelmän osassa sattuneen tuhon vaikutukset tulee voida välttää muualla tietojärjestelmässä. Elintärkeät toiminnot tulisi ylläpitää keskeytyksistä huolimatta mahdollisimman korkeatasoisesti.

Riippuvuus laajoista, verkottuneista tietojärjestelmistä on saanut aikaan olosuhteita, jotka eivät ole poikkeusoloja, vaikka niiden vaikutukset tietotekniikan kannalta ovat samanlaisia kuin poikkeusoloissa tapahtuvat vakavat tekniset häiriöt, yhteyskatkot ja keskeytykset. Tällaisiin erityistilanteisiin organisaation tulee varautua mutta niiden syntyyn se ei voi itse vaikuttaa. Varautuminen on tarpeen myös sellaisissa organisaatioissa, joilla ei ole poikkeusolojen valmiusvaatimuksia. Keskeytysten vaikutukset kohdistuvat yhä laajempaan asiakaskuntaan ja yhteistyötahoihin ja saattavat rajoittaa tai jopa estää tietojenkäsittelyn koko verkossa. Keskuslaitteympäristön ohella verkko-, tietoliikenne-, sähköposti- ja asiakaspalvelimien sekä tietoliikenneyhteyksien varmistaminen on välttämätöntä.

Palvelujen käytettävyysvaatimukset vaihtelevat tietojärjestelmien eri osissa. Palvelujen laadun ylläpitäminen vaatii usein jatkuvaa yhteyttä tietojärjestelmiin. Organisaatiot ovat yhä enemmän riippuvaisia toisten osapuolien käyttämistä tietojärjestelmistä. Korkeat vaatimukset asetetaan monille yritysten tuotanto- ja palvelujärjestelmille sekä valtion ja kuntien perustoimintoja kuten sairaanhoitoa ja energianjakelua ylläpitäville tietojärjestelmille.

Vioista ja onnettomuuksista aiheutuvien keskeytysten ohella vakavia uhkia aiheuttavat verkottuneessa tietojenkäsittelyssä suojaamattomiin järjestelmiin kohdistuvat hyökkäykset.

Varautuminen edellyttää valmiuksia palvelujen ja tietovarastojen eheyden säilyttämiseen, järjestelmien rakentamista vikasietoisiksi, luotettavaa varmuus- ja suojakopiointia sekä valmiita varajärjestelmäsuunnitelmia.

Toipumisvalmiuden arviointi

Toipumissuunnittelun lähtökohtana on keskeytyksiin johtavien uhkien ja toiminnan haavoittuvuuden tunteminen sekä näiden perusteella tehty selvitys ja arviointi tietotekniikkariippuvuuksista, toimintojen keskeytysriskeistä, keskeytysten vaikutuksista toimintaan ja tietojenkäsittelyn varmistamistarpeista.

Arvioinnin tuloksena määritellään:

- elintärkeät toiminnot ja palvelut
- elintärkeille toiminnoille ja palveluille välttämätön tietotekniikka
- tilanearviot vakaviin keskeytyksiin johtavista tapahtumista
- kriittisten tietojärjestelmien resurssitarpeet.

Toipumisvalmiuden arvioinnissa tarkasteltavia seikkoja on koottu liitteeseen 4c haavoittuvuuden arviointi, kohtaan toipumisvalmiuden arviointi.

Toipumisvalmiuden suunnittelu

Toipumissuunnitelmaan sisällytetään kaikki toimenpiteet, joita tarvitaan toiminnan jatkamiseen keskeytystilanteissa siihen asti, kunnes toiminta voidaan palauttaa alkuperäiselle käyttötasolle.

Suunnittelussa käsiteltäviä seikkoja ovat:

- tiedostojen varmistaminen
- elintärkeiden järjestelmien toiminnan varmistaminen
- varajärjestelmän käyttöympäristö laitteineen, ohjelmineen, yhteyksineen ja käyttötoimintoineen
- toipumissuunnitelmaan siirtyminen
- normaaliin tietojenkäsittelyyn palaaminen
- toipumisvalmiuden testaus.

Toipumissuunnittelussa käsitellään myös henkilöstöturvallisuuden, tietoaineistoturvallisuuden, laitteistoturvallisuuden, ohjelmistoturvallisuuden, tietoliikenneturvallisuuden, käyttöturvallisuuden ja fyysisen turvallisuuden varajärjestelmille asettamat vaatimukset. Organisaation toipumissuunnitelma voi muodostua useista erillistä tietojärjestelmäkohtaisista toisiinsa liittyvistä suunnitelmista.

Toipumissuunnitelman jäsentelystä on esimerkki liitteessä 5 tietoturvallisuuden suunnittelu, kohdassa toipumissuunnitelma.

Tiedostojen varmistaminen

Tietovaranto on yrityksen strateginen voimavara. Vakavissa fyysisissä vahinkotilanteissa sen tuhoutuminen voi johtaa koko organisaation toiminnan keskeytymiseen, ellei tietojen, tietojärjestelmien ja järjestelmädokumenttien kopioita voida käyttää palauttamiseen. Toipumisen perusedellytys on tietovarannon luotettava varmuus- ja suojakopiointi. Varmuskopio voi-

daan säilyttää käyttökohteessa. Säilytystilan tulee olla valvottu, palonkestävä ja tarvittaessa murtosuojattu tila. Suojakopiota säilytetään vastaavalla tavalla toisessa kiinteistössä. Sen päivitystiheys on määriteltävä tietojärjestelmäkohtaisesti. Suojakopio joudutaan säilyttämään lähellä käyttökohdetta tai muulla tavoin helposti saatavilla tuoreuden säilyttämiseksi, kun tapahtumatiheys on suuri. Olennaista on, että varmuuskopioidenkin tuhouttua suojakopiot voidaan päivittää saatavilla olevalla aineistolla riittävän lyhyessä ajassa. Suojakopio voi muodostua useista hajautetuista tietokannoista. Varmuus- ja suojakopioiden sisällön kattavuus on varmistettava säännöllisesti ja palautus testattava. Korkean käytettävyyden suojakopioarkistona on aiheellista käyttää tarkastettuja levyjä, joissa on käytettävyyden varmistavaa omaa logiikkaa.

Arkistolain mukaan arkistolaitos voi antaa määräyksiä valtion ja kuntien viranomaisille ja liikelaitoksille, julkisoikeudellisille laitoksille, seurakunnille sekä muille yhteisöille, toimielimille ja henkilöille, joille kertyy asiakirjojen julkisuudesta annetussa laissa tarkoitettuja asiakirjoja.¹⁹ Pitkäaikaisesti säilytettävällä nauhalla oleva aineisto on kopioitava toisille nauhoille viiden vuoden välein sekä luettava ja kelattava uudelleen vähintään kerran tällä kopiointivälillä.²⁰

Varajärjestelmä

Varajärjestelmän tarkoituksena on mahdollistaa keskeytyneen tietojärjestelmän tai tietojärjestelmien tukema toiminta, kunnes palaaminen alkuperäiselle palvelutasolle on taas mahdollista.

Varajärjestelmän laajuuteen vaikuttavat tuotannon ja palvelujen varmistustarpeet sekä keskeytyneen tietojärjestelmän ja verkkopalvelujen kokonaisrakenne. Osajärjestelmän vaurioituminen saattaa edellyttää varajärjestelmään liittyviä muutoksia vielä toimivissa tietojärjestelmän osissa. Toisaalta verkkopalveluissa syntyneet keskeytykset voivat johtaa varajärjestelmätarpeisiin useissa tietojärjestelmissä tai laajojen tietojärjestelmien osissa.

Omassa hallinnassa oleva varajärjestelmä on käytettävissä varmimmin. Sellaista tarvitaan erityisesti tärkeiden tuotannon ja prosessinohjauksen järjestelmien varmistamiseen. Varalaitteina voivat olla myös eri käyttäjien yhteiset varalaitteet tai palvelukeskuksen laitteet. Varajärjestelynä voi joissain tapauksissa olla manuaalinenkin järjestelmä.

Vaihtoehtoja ovat:

- jatkuvasti käytössä olevat rinnakkaiset laitteet
- muiden osajärjestelmien käyttö varalaitteina
- oma, erikseen luotava, valmisteltu varajärjestelmä
- sopimukseen perustuva palveluyrityksen varakeskus
- organisaatioiden yhteiset varalaitteet
- käyttöajan saanti toisten laitteistolta.

Ulkoistetun palvelun käyttäjän on asetettava varajärjestelmävaatimukset tietotekniikan palveluyritykselle samalla tavalla kuin perustettaessa omaa varajärjestelmää. Mikäli turvaututaan ulkomaisiin palvelukeskuksiin riippuvuus voi johtaa vaikeuksiin poikkeusoloissa.

Toipumissuunnitteluun kuuluu aina oleellisesti suunnitelma varajärjestelmän käyttöönotosta ja käytöstä sekä normaaliin tuotantoympäristöön pa-

laamisesta. Tämän suunnitelman mukaisesti voidaan suorittaa tarvittavien varajärjestelmien sekä niiden osien ja yhteyksien testaus. Testauksen tulee tapahtua ainakin vuosittain ja aina silloin, kun järjestelmää on muutettu. Sama koskee ulkoistettua varakeskuspalvelua. Testaus on valvottava ja tulokset dokumentoiva käyttöönottosuunnitelmaan.

Laitetoimittajien kanssa voidaan tehdä vaurioiden varalle sopimuksia laitteistojen toimituksesta tavanomaista lyhyemmillä toimitusajoilla. Toipumissuunnittelussa toimitus- ja kuntoonlaittoajat arvioidaan usein liian lyhyiksi.

Ohjelmistotoimittajat säilyttävät yleensä kopiot myymistään tai vuokraamistaan ohjelmatuotteista. Sopimuksin on varmistettava niiden käyttöön saanti tarvittaessa.

Joillekin tietojärjestelmille voidaan helposti ennalta luoda suppea, kokeemukseen perustuva tietokanta ja sovellus, jolla mikrotietokonetasoisesti voidaan hoitaa mm. säännöllinen laskutus-, palkka- ja muu sovellus sekä suorittaa tarkistusajo myöhemmin.

Varajärjestelmäkuvausten kopiot säilytetään suojakopioarkistossa.

Valtion atk-varakeskus

Valtion atk-varakeskuksen (VAVK) toiminta-ajatuksena on tarjota pääasiassa valtion tärkeille sovelluksille laitekapasiteettia ja käyttöympäristö poikkeusoloissa sekä erilaisissa äkillisissä katastrofitilanteissa toimimista varten. VAVK tarjoaa palveluja sekä keskuskone- että palvelinasiakkaille sekä rajoitetusti konesalipalveluja myös jatkuvasti käytettävissä oleville tuotantolaitteistoille. Sen toiminnasta ja kehittämisestä vastaa HVK. SFS Sertifiointi Oy on myöntänyt varakeskukselle tietoturvaluottamussertifikaatin.

Varalaitetilat

Koska tilojen rakenteelliset vaatimukset ovat korkeat, on varatila sitä tarvittaessa varattava ennalta ja valmisteltava ainakin sähköistys, ilmastointi, tietoliikenneyhteydet ja rakenteelliset muutokset.

Poikkeusoloissa tärkeän tietojärjestelmän varalaitteisto on sijoitettava toimintaan nähden tarkoituksenmukaisesti, mahdollisesti toiselle paikkakunnalle kuin varsinainen tuotantolaitteisto. Myös VAVK voi tarjota varalaitetilaa.

Tietoliikenteen ja verkkopalvelujen varmistaminen

Kaikille tärkeille verkoille on laadittava toipumissuunnitelmat, jotka testataan kokeiluina tai varajärjestelmän toimintaa jäljitellen. Muiden hallinnassa olevat varmistamattomat verkkojen ja tietoliikenteen solmukohtat ovat kriittisimpiä tietojärjestelmien osia. Arkoja ovat myös ne reitit, joille ei ole vaihtoehtoisia yhteyksiä. Tällaisia ovat mm. kiinteistöstä dataverkon solmuun johtavat paikallisyhteydet. Solmun jälkeen varareititys on mahdollista.

Tietoliikenteen ja verkkopalvelujen varmistaminen edellyttää:

- verkkoriippuvuuksien ja niistä aiheutuvien riskien tunnistamista
- elintärkeiden tietojärjestelmien tarvitsemien verkkoyhteyksien arviointia

- verkko-operaattorien valmiuksien tuntemista
- tietoliikenneverkkojen solmukohtien varmistamista
- tarvittaessa paikallisyhteyksien kahdentamista
- tietoliikenneyhteyksien luomista ja ohjaamista ehjistä järjestelmänosista varajärjestelmään
- tiedonkeruun vaatimien varayhteyksien järjestämistä
- verkon laitteiden varmistuksia ja varaosia
- yhteistoimintaa ja tarvittaessa sopimuksia tietotekniikan palveluyritysten ja operaattorien kanssa.

Tiedonsiirtoyhteyksien varaukset ja osoitteet valmistellaan ennalta verkon omistajan kanssa ja vahvistetaan sopimuksin.

Verkkojen pirstoutuminen eri operaattorien käyttöön ja operaattoreiden toiminnassa tapahtuvat muutokset on pyrittävä ottamaan huomioon seurannassa ja suunnitelmien päivityksessä.

Varavoiman saannin varmistaminen

Tärkein tietotekniikan perusrakenne on sähköverkko. Hajautetussa verkossa tietojenkäsittelyn eheys edellyttää luotettavaa virransyöttöä kaikkiin kriittisen järjestelmän osiin. Tärkeiden tietoteknisten keskusten virransyöttö on varmistettava kahdesta eri muuntajapiiristä. Katkottoman virransyötön (UPS) laittein voidaan virransyöttö varmistaa enintään muutamiksi tunneiksi. Kriittisten järjestelmien jatkuva sähkönsaanti on näin ollen varmistettava omin varavoimakonein. Tämä taas edellyttää niitä varten varattuja tiloja ja polttoaineen saannin varmistamista.

Lähiverkot

Lukumääräisesti eniten tietojenkäsittelyä häiritsevät lähiverkon palvelimissa sattuvat häiriöt ja ympäristekniikan viat. Työasemajärjestelmän keskeytykset aiheuttavat ulkoisille ja sisäisille asiakkaille tarjottavien palvelujen keskeytymisen.

Lähiverkkojen varajärjestelmätarpeeseen vaikuttavat käytettävyystarpeet, työasemaverkossa tarjottujen palvelujen laatu, käyttäjien määrä ja järjestelmän merkitys tietojenkäsittelykokonaisuuden osana. Häiriöiden varalta palvelimet on varmistettavissa rinnakkaisin levyin tai rinnakkaisin palvelimin. On huomattava, ettei keskuslaitte- ja palvelintilojen vaurioituessa pelkkä paikallinen levyvarmistus riitä vahingon vaikutuksilta suojautumiseen. Tärkeiden keskuslaitteiden ajantasainen suojakopio on varmistettava toisessa kiinteistössä sijaitsevin korkeatasoisin levyin. Palvelimien toiminnan varmistaminen edellyttää suunnitelmaa teknisten järjestelmien varalaitteistojen kuten UPS-laitteen käyttöönotosta.

Vakavassa kiinteistön turossa koko työasemaverkon käyttö estyy. Toiminnan jatkamiseksi on tietojenkäsittely siirrettävä muualle. Usein on parasta suunnitella ja valmistella välttämättömän tietojenkäsittelyn siirto toiseen, esimerkiksi rinnakkaisen yksikön työasemaverkkoon. Siirtymisen tulee tapahtua hyvin testattuna ja harjoiteltuna rutiinitoimenpiteenä. Toimeenpanon vastuuhenkilöiden tulee olla nimettyjä ja sijaisuudet järjestettyjä.

Sähköposti

Sähköposti on ratkaisevan tärkeä informaatioväline. Siihen tukeutuvat johtamistoiminnot, tärkeä informaation välitys sekä monet palvelut ja toimin-

tojen ylläpito. Sähköpostijärjestelmän häiriöttömän toiminnan varmistamiseen on kiinnitettävä erityistä huomiota. Sähköpostijärjestelmän varapalvelin ja verkkoyhteydet on kyettävä ottamaan käyttöön hyvin lyhyessä ajassa vioittuneen sähköpostijärjestelmän korvaamiseksi.

Sähköpostin virustarkistuksista huolimatta käytössä on varauduttava virus-tartunnan seurauksena postijärjestelmän täydelliseen sulkemiseen tartunnan ajaksi ja tärkeimmän tiedonsiirron hoitamiseen muilla välineillä.

Toipumissuunnitelmaan siirtyminen

Varajärjestelmään siirtyminen, henkilöstön toiminta, laitteiston käyttö ja normaalitoimintaan palaaminen suunnitellaan toimivaksi kokonaisuudeksi.

Toipumissuunnitelman käynnistämisen periaatteet ovat:

- toiminnan palautumista odotetaan, ellei siitä aiheudu merkittäviä vahinkoja ja menetyksiä
- jos vahingot ovat merkittäviä, niitä vähennetään keskittymällä kriittisten sovellusten hoitoon
- ellei palautuminen onnistu asetetuissa aikarajoissa, tehdään päätös toipumissuunnitelman käynnistämisestä ja siirtymisestä varajärjestelmään.

Suunnitelmassa pitää esittää, mitkä tietojärjestelmät pystytetään ja miten keskeytyneiden tietojärjestelmien osatoiminnot korvataan.

Varajärjestelmien käyttöönottoon tarvitaan ennalta koulutettu valmiusryhmä, jonka tehtävänä varajärjestelmään siirryttäessä on:

- tarvittava henkilöstön hälyttäminen
- varajärjestelmän käynnistykseen tarvittavan aineiston ja välineistön koostaminen sekä varajärjestelmän kunnostuksen valvonta
- varajärjestelmäsopimusten toimeenpano
- tarvittavien yhteyksien järjestäminen
- tarvittavien kuljetuksien järjestäminen
- toipumisen edellyttämien toimenpiteiden käynnistäminen kuten huollon, laitteiden ja tilojen hankkiminen ja kunnostaminen
- varakeskuksen pystytys, yhteydet, käynnistys, toiminnan testaus ja tuotantokäyttö.

Valmiusryhmään nimetään käytön tuntevat, siitä vastaavat ja muutenkin varmistettavassa käyttöympäristössä sitä hoitavat henkilöt. Suunnitelmassa nimetään valmiusryhmän johtaja, vastuuhenkilöt sijaisineen, muu varajärjestelmän vaatima henkilöstö sekä johdon ja ao. yksiköiden toiminnasta vastuulliset esimiehet.

Palaaminen normaaliin toimintaan

Varajärjestelmän suunnittelun yhteydessä määritellään normaalitoimintaan palaamisen periaatteet ja valmistelutehtävät. Ensisijaista on menetettyjen laitteistojen uusiminen niin, että varajärjestelmän käyttö jää mahdollisimman lyhyeksi.

Toipumissuunnitelman testaus

Toipumissuunnitelman testaus käsittää

- toipumissuunnitelman tarkastuksen
- häilytyksien suorittamisen erilaisissa ongelma- ja keskeytystilanteissa
- varmuus- ja suojakopioiden päivityksen, säilytyksen, kattavuuden ja lukukelpoisuuden tarkistuksen
- sopimusten tarkastuksen
- laitteiden toimitusaikojen tarkastuksen
- elintärkeiden järjestelmien priorisoinnin tarkastuksen
- valittavassa laajuudessa varajärjestelmän testauksen ns. pöytätestein tai suorittamalla testauksen käytännössä
- tietoliikenteen varayhteyksien tarkastuksen ja testauksen
- mahdollisten manuaalisten osajärjestelmien tarkastuksen ja testauksen
- puutteiden ja lisätoimenpiteiden kirjaamisen
- arvioinnin valmiudesta vakaviin keskeytystilanteisiin
- päätökset korjausten toteuttamisesta.

Varajärjestelmät voidaan testata ja toipumissuunnitelmat tarkistaa myös katastrofiharjoituksena. Mikäli järjestelmän testaus on laiminlyöty, menevät siihen uhratut investoinnit ja työpanokset hukkaan. Varajärjestelmän tulee olla loppuun asti suunniteltu ja harjoiteltu. Apua ei enää löydy varsinkaan silloin, kun erityistilanteet kohdistuvat myös muihin.

Seuranta

Toipumissuunnitelma pysyy käyttökelpoisena, kun tietojärjestelmien muuttumista seurataan jatkuvasti ja päivitetään sitä tarpeen mukaan. Suunnitelmien ylläpito on toimintojen johdon ja tietojärjestelmien omistajan vastuulla. Toipumissuunnitelma päivitetään aina tietojenkäsittelyssä tapahtuvien muutosten yhteydessä ja vähintään vuosittain.

Tiedottaminen

Keskeytykset aiheuttavat lähes aina muutoksia tietojärjestelmien käyttöön sekä ulkoisten ja sisäisten asiakkaiden toimintoihin. Toipumissuunnittelussa valmistellaan muutoksista tiedottaminen. Kriisitiedottamiseen varautuminen ja sen valmistelu voi olla välttämätöntä vakavien, laajavaikutteisten vahinkotilanteiden varalta. Keskeytykset saattavat johtaa yrityskuvan huonontumiseen ja asiakasmenetyksiin, ellei vaikutuksia lievennetä tiedottamalla ohjaustoimista.

Toipumissuunnitelman säilytys

Toipumissuunnitelma on valmiusryhmän käsikirja vakavissa keskeytystilanteissa. Ainakin yksi kopio siitä säilytetään suojakopioarkistossa kiinteistön ulkopuolella.

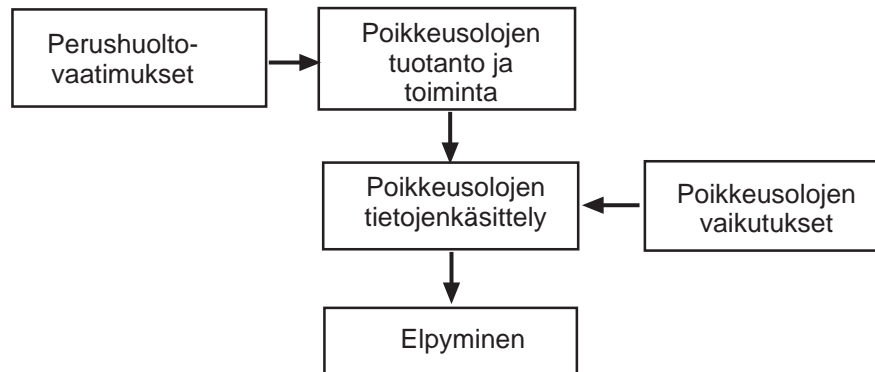
Toipumissuunnitelma (esimerkki)

Sisältö:

- Elintärkeiden toimintojen, tietojärjestelmien ja sovellusten määrittely, varmistettavat palvelut
- Elintärkeille toiminnoille määritellyt suurimmat sallitut keskeytysajat
- Sähköisten palvelujen varmistaminen
- Kuvaukset vakavaan keskeytykseen johtavista tapahtumista
- Kuvaukset erityistilanteiden vaikutuksista toimintaan
- Varajärjestelmäratkaisut
 - laitteet
 - varatilat
 - varavoiman turvaaminen
 - korjauksen ja uuden laitteiston toimitukset
 - tiedonsiirto
 - verkkopalvelut ja niiden varmistaminen
 - sähkö- ja teleliitännät
 - välttämättömien manuaalitoimenpiteiden varmistaminen
- Valmiusorganisaatio
 - vastuut toipumissuunnitelman käynnistämisestä ja toimenpiteistä
 - vastuuhenkilöiden hälyttäminen
 - yhteyshenkilöt (laitetoimittaja, huolto, varajärjestelmän omistaja, vakuutusyhtiö)
- Toimenpiteet
 - varmuus- ja suojakopiointi ja käytön varmistaminen
 - ohjeet laitteiden, ohjelmistojen, tiedostojen ja tarvikkeiden pelastamisesta
 - muut vahingon rajoittamismenettelyt
 - varajärjestelmän käynnistysjärjestys
 - suojakopioiden ja ohjelmistosiirron suoritus
 - siirtosuunnitelma varatilaan tai varajärjestelmään siirtymiseksi
 - varajärjestelmän turvallisuustoimenpiteet
 - tiedottaminen ja asiakkaisiin liittyvät toimenpiteet
 - normaalijärjestelmään palautumisen edellyttämät hankinnat, kunnostus- ja toimitussopimukset
 - toiminnan uudelleenkäynnistys ja tietojärjestelmien kunnostus
 - järjestelmän testaus palautumisen jälkeen
- Ulkoistettujen järjestelmäpalvelujen varmistaminen
- Keskeytysvakuutukset
- Koulutus
- Toipumissuunnitelman ylläpito, testaus ja päivitys
- Raportointi johdolle

7. POIKKEUSOLOJEN VALMIUSSUUNNITELMA

Poikkeusolojen tietojenkäsittelyn reunaehtoina on perushuoltovaatimuksesta tai organisaation omista lähtökohdista johdetut vaatimukset tuotannolle ja toiminnalle sekä toisaalta poikkeusolojen vaikutukset toimintaan ja tietojenkäsittelyyn. Nämä tekijät sanelevat tietojenkäsittelyn valmiusvaatimukset.



7.1 Poikkeusolojen valmiussuunnittelun perusteet

Tietojenkäsittelyn poikkeusolojen valmiussuunnittelun tavoitteena on poikkeusolojen vaikutusten tunnistaminen ja organisaation poikkeusoloissakin välttämättömän tietojenkäsittelyn varmistaminen vakavissa ulkoisissa kriisitilanteissa. Omien jatkuvuusvaatimusten ohella poikkeusolojen tietojenkäsittelyn perusteena on virastojen, laitosten ja yritysten merkitys poikkeusoloissa. Tärkeysluokittelu on eräs tavoiteasettelun lähtökohta.

Poikkeusolojen valmiuden perustana on normaaliolojen turvallisuus - perusturvallisuus. Tietoturvaluussuunnitelman tietoturvaluusustoimenpiteet korostuvat poikkeusoloissa, toipumissuunnitelmat antavat perusteita poikkeusolojen valmiussuunnitteluun, vaikka varmistamistarpeet ovatkin erilaiset. Poikkeusoloissa tietojenkäsittelyn mahdollisuuksissa, organisaatioissa ja toimintatavoissa tapahtuu niin jyrkkiä muutoksia, että suunnitelmat on laadittava näihin erikseen.

Poikkeusolojen tietojenkäsittelyä voidaan kuvata vaiheittaisena siirtymisenä nykyisistä järjestelmistä alemmalle käyttötasolle. Ainakin tärkeimmät toiminnot pyritään hoitamaan tietojärjestelmin kaikissa poikkeusoloissa. Valmiussuunnitelmalla sopeutetaan tietojenkäsittely kriisitilanteisiin sopivaksi. Tietotekniikan palvelu- ja huoltoyritysten on tuettava tärkeiden asiakkaiden varautumista. Kotimaisen osaamisen merkitys kasvaa.

Poikkeusolojen tietotekniikka voi pohjautua toipumissuunnittelussa tehtyihin varajärjestelmäratkaisuihin lukuun ottamatta organisaatioita, joissa toiminnan ja tuotannon luonne poikkeusoloissa muuttuu ja muuttaa myös tietojärjestelmiä.

7.2 Lähtökohdat

Poikkeusolojen valmiussuunnittelun lähtökohtia ovat:

- johdon saama kokonaiskuva poikkeusolojen vaikutuksista, tärkeysluokituksesta ja valmiussuunnittelusta vastaavien viranomaisten vaatimuksista ja odotuksista
- johdon päätökset poikkeusolojen tuotannosta ja toiminnasta
- päätökset organisaation tehtävistä ja valmiuden tasosta
- valmiussuunnittelun käynnistäminen johdon nimeämän vastuuhenkilön/valmiuspäällikön johdolla.

Tietojenkäsittelyn valmiustavoitteita määriteltäessä on ratkaistava:

- mitä organisaation poikkeusolojen toiminnalta, tuotannolta ja palveluilta odotetaan
- miten organisaatio haluaa toimia kriisitilanteissa
- mitkä ovat toimipaikkojen ja tuotantoyksiköiden valmiustavoitteet
- mitkä ovat poikkeusolojen vaikutukset toimintaan
- mitä tiedonsiirron resursseja ja palveluita tarvitaan
- mitkä valmiustavoitteet on asetettava tietojenkäsittelylle ja sen osille vaatimusten täyttämiseksi.

Poikkeusolojen valmiuden arvioinnissa tarkasteltavia seikkoja on koottu liitteeseen 4c haavoittuvuuden arviointi, kohtaan tietojenkäsittelyn poikkeusolojen valmiuden arviointi.

Valmiussuunnitelman tulee pohjautua tosiasioihin perustuvaan arvioon toimintamahdollisuuksista poikkeusoloissa silloin, kun

- ulkomaiset verkkoyhteydet eivät toimi
- sähköjakelussa esiintyy usein ja pitkiä häiriöitä
- ulkomaiset tietoliikenneyhteydet ovat poikki
- kotimaiset tietoliikenneyhteydet ovat poikki tai
- paikallistasolla tietoliikenneyhteydet ovat häiriöiset.

Tietotekniikan palveluyrityksellä ei ole suoria varautumisvelvoitteita. Palvelun tilaajan on sovittava palvelusopimuksella valmiusjärjestelyistä palveluyrityksen kanssa. Palveluyritys voi luoda vaadittavan teknisen valmiuden sopimuksen edellyttämässä laajuudessa. Luonnollisesti vastuu poikkeusolojen valmiudesta on kuitenkin palvelun tilaajalla.

Palvelusopimukseen sisällytetään poikkeusolojen valmiutta varten:

- poikkeusoloissa ylläpidettävät tietojärjestelmät
- varmistettavien järjestelmien tiedot
- käyttöympäristön, laitteiden ja tietoliikennepalvelujen määrittely
- yhteyshenkilöt
- käyttöönotto-oikeudet
- tietovarastot
- toimintatilat
- valmiuden kohottaminen
- järjestelmän miehittäminen, käyttöhenkilöstön varaukset
- ohjelmistot
- käytön erityisohjeet, tietoturvallisuuden valvonta ja raportointi

- varaosat ja varattava muu materiaali
- turvallisuusjärjestelyt ja -vaatimukset
- menettelyt valmiussuunnitelman laatimiseksi ja ylläpitämiseksi
- muut velvoitteet osapuolille
- taloudelliset sopimusehdot.

Poikkeusolojen valmiussuunnittelussa on arvioitava myös verkko-ope-
raattorien poikkeusolojen valmius ja tehtävä tarvittavat sopimukset mah-
dollisuuksien mukaan.

Poikkeusolojen valmiussuunnitelman jäsentelystä on esimerkki liitteessä 5
tietoturvallisuuden suunnittelu, kohdassa tietojenkäsittelyn poikkeusolojen
valmiussuunnitelma.

7.3 Poikkeusolojen vaikutusten arviointi

Tietojenkäsittelyn kannalta poikkeusolojen häiriöt kohdistuvat pahimmin
tietoliikenteeseen, henkilöstöön, laitteistoihin ja huoltoon.

Toimintaedellytyksiin vaikuttavat mm.:

- ulkomaisten tietoliikenneyhteyksien lamaaneminen tai katkeaminen
- tukeutuminen pääasiassa kotimaisiin resursseihin ulkomaisten tietotek-
niikkapalvelujen käytön rajoituksessa jyrkästi
- valmiuslain perusteella valtioneuvoston saamat valtuudet valvoa ja
säännöstellä muun muassa tietoteknisten laitteiden ja palvelujen, vara-
osien ja huoltopalvelujen käyttöä
- organisaation ennalta varaamattomien henkilöiden kutsunta kertaushar-
joituksiin tai olosuhteiden vaatiessa ylimääräiseen palvelukseen
- valmiuslain perusteella velvoitteet tavaroiden sekä työ- ja palvelusuori-
tusten luovutukseen
- puolustustilalain voimassa ollessa velvoitteet tavaroiden luovutukseen
sotilaalliseen maanpuolustukseen tai sotatalouden käyttöön ja työvelvol-
listen käyttö työvelvollisuuslain suomin valtuuksin valtioneuvoston
päättämällä aloilla.

Säännöstelyviranomaisena toimii VM:n yhteyteen perustettava tiedonkä-
sittelyn säännöstely-yksikkö (TSY). Viranomaisen säännöstellessä tietotek-
niikan käyttöä voidaan organisaation laitteistolle osoittaa muiden orga-
nisaatioiden tietojenkäsittelytehtäviä tai ottaa laitteisto viranomaisten
käyttöön. Tämä saattaa vähentää huomattavasti omaan käyttöön jäävää
tietotekniikkaa.

Avoimiin verkkoihin perustuvat järjestelmät voidaan halvaannuttaa ainakin
ajoittain ja paikallisesti. Uhka lisääntyy jatkuvasti sähköisen liiketoimin-
nan ja verkkojen ohjauksen siirtyessä avoimiin järjestelmiin.

Haitan- ja vahingonteko laajenee todennäköisesti nopeasti poikkeusoloissa.
Vihamielinen taho voi sabotoida toimintaa vaikuttamalla tietojenkäsittelyyn
jo ennen kriisin puhkeamista, tuholaistoiminnalla, häiritsemällä tietoliiken-
nettä, tunkeutumalla tietojärjestelmiin, sieppaamalla tietoa, syöttämällä
harhauttavaa tietoa tai estämällä tiedon kulun. Uusi teknologia lisää
elektronisen häirinnän ja tuhoamisen riskiä. Häirintäriskit riippuvat myös
organisaation toiminnan luonteesta. Poikkeusoloissa riskit kasvavat yhti-
teiskunnallisesti tärkeissä organisaatioissa, tuotantolaitoksissa ja tietoliik-
kenneverkon ylläpidossa.

7.4 Kriittiset järjestelmät

Poikkeusoloissa organisaation toiminta ja tuotanto muuttuu asetettujen tehtävien ja velvoitteiden mukaan. Samalla myös tietojärjestelmien merkitys voi muuttua. Tietojärjestelmille asetettavat toiminta- ja käyttövaatimukset perustuvat toimintaprosesseille asetettaviin valmiustavoitteisiin. Normaalioloja varten laadittu tietojärjestelmien tärkeysluokitus tulee tarkastaa silmällä pitäen poikkeusolojen valmiussuunnittelua.

Seuraavaa ryhmittely on yleisohje, jota valmiussuunnittelussa voidaan soveltaa organisaatiolle sopivaksi.

1. ryhmään kuuluvat sellaiset tietojärjestelmät ja sovellukset, joiden tuemat toiminnot ovat välttämättömiä poikkeusoloissa, kuten kansalaisten toimeentulon, maan elinkeinoelämän tai maanpuolustuksen kannalta välttämätön tuotanto ja palvelut sekä edellä mainittujen järjestelmien ylläpitämiseen ja varmistamiseen tarvittavat järjestelmät ja palvelut.

2. ryhmään kuuluvat sellaiset sovellukset, joiden toimintaa supistetaan poikkeusoloissa ja joissa tietotekniikan käyttöä voidaan supistaa.

3. ryhmään kuuluvat sellaiset sovellusalueet, jotka voidaan korvata tai lopettaa.

Poikkeusolojen tietojenkäsittelyn palvelusovaatimukset eritellään tietojärjestelmittäin. Poikkeusolojen tietojärjestelmien resursseista ja niiden ylläpidosta laaditaan yhteenveto ja optimoidaan tarpeet sekä määritellään tietojärjestelmille jaettavat resurssit, kuten henkilöresurssit, laitteet, varalaitteet, tietoliikenne, erikoismateriaali, tarvikkeet, huolto ja ylläpito.

7.5 Laitteet, varaosat, tarvikkeet ja huolto

Kuljetusten lamaantuminen, kauppasaarto tai ulkomaiden vientikiellot voivat pysäyttää kaiken tietoteknisten laitteiden, varaosien, tietovälineiden ja tarvikkeiden tuonnin maahamme. Kansallisten varastojen loppuessa toimivien laitteiden määrä laskee nopeasti ja osaa niistä joudutaan käyttämään varaosina. Pelkästään suurvaltojen välisten suhteiden häiriytymisen tiedetään vaikuttavan logistiikkaketjujen toimintaan ja tietoteknisten laitteiden saantiin ja huoltoon. Elektroniikkakomponentit saattavat strategisena materiaalina joutua valmistajamaassa vientikieltoon.

Poikkeusoloissa tietojenkäsittelyä jatketaan alkuperäisillä laitteistoilla ottaen huomioon toiminnan supistukset. Varalaitteita joudutaan ottamaan käyttöön ja varajärjestelmiin siirrytään jo laiterikkojenkin seurauksena.

Laitteiden hankintaperiaatteilla vaikutetaan laitteiden, ohjelmistojen ja sovellusten yhteensopivuuteen, huoltopalvelujen ohjaukseen ja varaosien saantiin eriasteisissa kriiseissä. Poikkeusolojen tietojärjestelmistä on tehtävä päätökset ja palattava tarvittaessa aikaisempiin, yksinkertaisempiin käyttötapoihin, omaan korjaustoimintaan ja vapautuneiden laitteiden käyttöön.

Tietoteknisten laitteiden ja tarvikkeiden varastointia on vaikea järjestää, koska nopea tekninen kehitys muuttaa tarpeita. Poikkeusoloissa varalaitetarpeet turvataan pääasiassa viranomaisten ohjauksella ja säännöstelyllä.

On kuitenkin tärkeää, että organisaatiot pitävät kriittisimmistä tarvikkeista tavanomaista tarvetta suurempaa välivarastoa, sillä jakelukeskukset sijaitsevat yleensä ulkomailla.

Kriittisiä tarvikkeita ovat mm.:

- palvelimien kiintolevyt, emolevyt ja verkkokortit
- työasemien tavallisimmat varaosat ja tarvikkeet
- keskitimet, keskitinkortit ja reitittimet
- nauhat ja levykkeet
- verkon rakennusmateriaalit
- massatulostimien varaosat, tarvikkeet, värikasetit ja kirjoittimien tarvikkeet
- erikoistarvikkeet.

Turvavarastointia koskevan lain perusteella yrityksillä on mahdollisuus saada tietotekniikan varaosien ja -tarvikkeiden varastointiin valtion korkotukea ja varastointiavustusta.²¹

Poikkeusoloissa laitehuolto vaikeutuu, kun ulkomaista tukea ei saada, kaukodiagnostiikkaa ei voida käyttää ja huollon henkilöresurssit vähenevät. Säännöstelyn seurauksena jäävät vähemmän tärkeät tietotekniset laitteet ilman huoltoa. Parhaiten huollon saatavuuden voi taata oma huoltohenkilöstö, varaosavarastot ja omien vapautuvien laitteiden käyttö. Tietotekniikan huoltoyrityksen toimintamahdollisuuksista on aiheellista varmistua ennen tärkeän huoltosopimuksen hyväksymistä. Säännöstelyn vallitessa voidaan huoltajaksi osoittaa myös joku muu kuin normaalioloissa käytetty huoltoyritys. Huoltosopimukseen sisällytetään organisaation vaatimat erityistarpeet kuten varalaitetoimitukset, huollon saatavuus eri tilanteissa tai organisaatiolle varattava poikkeuksellinen varaosavarasto.

Tietotekniikan kustannusraportoinnista saa tarpeellista tietoa tärkeiden sovellusten vaatimista resursseista myös varakonesopimuksiin ja poikkeusolojen tarpeisiin.

7.6 Tietoliikenne

Viestiverkkoihin, niiden laitteisiin tai keskuksiin vaikuttava tai kohdistuva suuronnettomuus, terroritoiminta ja sotatoimet saavat aikaan fyysisiä vaurioita, joiden korjaaminen kestää jopa viikkoja. Häiriötilanteissa liikenteen ruuhkautuminen voi tukkia puhelinverkon pitkäksi ajaksi. Kauan kestänyt taloudellinen kriisi vähentää viestiverkon käytettävyyttä kunnossapitoon tarvittavan materiaalin loppuessa. Sodanuhkavaiheesta lähtien osa viestiyhteyksistä jouduttaneen luovuttamaan puolustusvoimien, väestönsuojelun ja muiden viranomaisorganisaatioiden käyttöön. Tietoliikenneyhteyksien häirintä ja salakuuntelu on todennäköistä.

Sodan aikana viestiyhteydet ja niihin liittyvät laitteet ja laitokset ovat todennäköisiä tuhoamiskohteita. Tiedonsiirrossa on valmistauduttava tietovälinekuljetuksiin ainakin pahimpien kriisien aikana. Varatiloihin siirrettävän laitteiston yhteydet on valmisteltava ennalta ja tehtävä tarvittavat yhteysvaraukset telelaitoksilta. Matkaviestinverkoissa hoidettavat, toiminnalle tärkeät yhteydet vaativat varmistamista muita yhteysmuotoja käyttäen, sillä poikkeusoloissa ei radiotaajuudella toimivien verkkojen häirinnältä voida suojautua.

Tiedonsiirron suunnittelun perusteiksi selvitetään poikkeusolojen tietojenkäsittelyn tiedonsiirtoriippuvuus ja tiedonsiirtomahdollisuudet sekä varmistukset. Suunnitelmissa varaudutaan vakaviin yhteyskatkoihin. On epärealistista luottaa yleisen tietoverkon käyttöön kaikissa poikkeusoloissa. Tärkeysluokiteltujen organisaatioiden tulisi käyttää sellaisia tunnettujen operaattoreiden verkkopalveluja, joilla voidaan taata toiminnan jatkuvuus. Tietoliikenteen suunnittelussa asetetaan vaatimukset käytettävien yhteyksien laadulle ja suojaamiselle, kiinteiden yhteyksien tarpeelle, yhteyksien varmistukselle ja salaukselle sekä valitaan järjestelmäkohtaisesti tiedonsiirtotavat.

Verkkojen hallinnan varmistamiseksi hallintakeskukset on pyrittävä kahdentamaan ja verkonhallintayhteydet hajauttamaan, salaamaan ja varmentamaan. Internetiin perustuvissa, valtakunnan rajat ylittävissä yhteyksissä on verkonhallinta varauduttava varmentamaan päästä päähän. Verkkoperaattorien tulee valmiussuunnitelmissaan selvittää toimintaansa kohdistuvat uhat ja tietoliikenteen varmistamisen taso siten, että se palvelee tärkeiden asiakkaiden poikkeusolojen valmiussuunnittelua ja sen perustaksi tehtäviä ratkaisuja.

7.7 Logistiikka ja kuljetukset

Poikkeusoloissa kuljetuksiin kohdistuu häiriöitä, jotka rajoittavat ja epä-säännöllistävät kuljetuksia. Lisäksi viranomaisen valvoo ja säännöstelee liikennettä, kuljetuksia ja kuljetusvälineiden käyttöä. Tämän vuoksi poikkeusolojen kuljetukset vaativat suunnittelua ja valmistelua.

Kuljetusten valmiussuunnitelma laaditaan tuotantotoiminnan valmiussuunnitelman yhteydessä. Tämä suunnitelma sisältää poikkeusolojen tuotannon, varastoinnin, materiaalien ja polttoaineiden kuljetustarpeet sekä kuljetuksen järjestelyt.

Tietojenkäsittelyn valmiussuunnittelussa kiinnitetään huomiota jakelukuljetusten logistiikan ja tuotannon materiaalivirtojen ohjauksjärjestelmien varmistamiseen poikkeusoloissa.

7.8 Henkilöstö

Vastuujärjestelyt

Poikkeusolojen toimintaorganisaatio perustuu normaaliolojen käytäntöön. Henkilöstöön kuitenkin vaikuttavat mm. tuotannon muutokset sekä puolustusvoimien kutsunnat ja väestönsuojelun henkilöstötarpeet.

Yksiköiden johdon ja tietohallintojohdon tehtäviä täydennetään tietojenkäsittelyn valmiussuunnittelu- ja turvallisuusvastoilla.

Kriisitilanteiden käyttöorganisaatio on välttämättömien sovellusten henkilöstöstä koottu perusryhmä, jolla organisaation tietojenkäsittely pidetään toiminnassa poikkeusoloissa. Käyttöorganisaation tulee olla toimintakykyinen myös liikekannallepanon jälkeen, joten sen henkilövarauksista tulee huolehtia. Ryhmän jäsenten tulee edustaa hallinnon, käytön (myös mahdollisilla varakoneilla), tietoliikenteen, tärkeimpien sovellusalueiden, tietotekniikan huollon, LVI-huollon, sähköhuollon, fyysisen turvallisuuden, kuljetuksien ja henkilöstöhallinnon asiantuntemusta.

Henkilövaraukset

Asevelvollisten kutsunnan vaikutusta on usein vaikea kuvitella, vaikka sen aiheuttamalla henkilöstön vähenemisellä on vakavissa kriisitilanteissa suuri merkitys organisaatioiden toimintaan. Välttämättömän toiminnan ylläpitämiseksi voi organisaatio varata asevelvollista henkilöstöä (ns. VAP-varaukset) omaan käyttöönsä, mikäli sen toiminta on tärkeää väestön toimeentulolle, välttämättömän talouselämän jatkumiselle, maan taloudelliselle puolustusvalmiudelle, puolustusvoimien varustamiseksi tai estämään yleisiä etuja joutumasta vaaranalaiseksi.²²

Henkilövaraus tapahtuu anomalla nimettyjä henkilöitä vapautettaviksi asevelvollisuuden suorittamisesta sodan aikana. Esitys tehdään sen sotilaslääkinnän esikunnalle, jonka alueella organisaation päätoimipaikka on. Vapautettuja ei yleensä kutsuta kertausharjoituksiin. Varauksia voivat tehdä myös laitetoimittajat, palvelukeskukset ja huoltoyritykset asiakkaidensa tärkeyden ja tarpeiden perusteella. Puolustusvoimien varauspäätökset ovat voimassa toistaiseksi. Kriisin syvetessä voidaan palvelukseen kutsua myös niitä, joiden varaukset on hyväksytty.

Henkilöstön varaus suunnitelmassa määritellään tietojenkäsittelyn vaatimat henkilöresurssit henkilöryhmittäin. PTS ja pääesikunta ovat laatineet ohjeen tietotekniikka-alan avainhenkilöstön varaamisesta.²³

Huolimatta varausmahdollisuudesta on valmiusorganisaatioon pyrittävä sijoittamaan ei-asevelvollista henkilöstöä ja suunniteltava korvaavan henkilöstön koulutus poikkeusolojen tehtäviin.

Sotilaslääneistä on saatavissa ohjeita yrityksiä asevelvollisten henkilöiden varaamiseen liittyvissä käytännön kysymyksissä. Henkilövaraukset liitetään henkilöstöhallinnon rutiineihin ja valmiuspäällikön tekemiin muihin varausesityksiin.

Poikkeusoloissa henkilöstön käyttöön vaikuttavat myös työvoimapula ja vaikeissa kriiseissä henkilötappiot.

Koulutus

Täydennyskoulutusta suunnataan myös valmiuden ylläpitämiseen. Koulutustarpeen aiheuttaa mm. tietotekniikan oman osaamisen säilyttäminen, sijaisjärjestelyt, muuttuvat työt ja valmiuden luominen. Turvallisuustoiminnan koulutussuunnitelmat täydennetään kattamaan valmiustehtävät.

Kohotettaessa valmiutta on sijaisten täydennyskoulutus aloitettava välittömästi. Jokaiselle valmiustehtäviin sijoitetulle asevelvolliselle on myös nimettävä seuraaja ja myös tätä on koulutettava.

7.9 Ohjelmistot ja käyttö

Poikkeusoloissa käyttötoimintaan vaikuttavat :

- muutokset toiminnassa ja tietojenkäsittelyssä
- tietoturvallisuustarpeiden muutokset
- ongelmat järjestelmien eheyden ylläpidossa
- tiedonsiirtoyhteyksien ja -laitteiden häiriöiden aiheuttamat ongelmat tiedonsiirrossa ja erityisesti järjestelmien eheyden ylläpidossa

- henkilöstön vähetessä järjestelmä- ja ohjelmointityön vaikeutuminen, osaamisen puutteet, tukipalvelujen kaventuminen
- ohjelmistojen vaurioitumisriskien lisääntyminen
- jatkuvan varmuus- ja suojakopioinnin merkityksen lisääntyminen
- valtakunnan kannalta tärkeiden tiedostojen tietosisällön suojaamistarpeiden kasvu ja
- tiedonsiirron lamaantuminen, tietovälineiden kuljetusten lisäys.

Tietoturvallisuuden vaatimusten kasvaessa myös tapahtumien havainnointia on tarkennettava ainakin sellaisissa järjestelmissä, jotka ovat tärkeitä maan turvallisuuden kannalta. Valvojalle on ilmoitettava, mikäli toiminta on virheellistä, luvaton tai rikkoo turvallisuusrajat. Mm. luvaton päätteen tai tiedoston käyttöyritys, tunkeutumisyritykset verkkoon ja tietokantoihin ja tulostaminen kiellettyyn osoitteeseen edellyttävät ilmoitusta. Tietojärjestelmien suojausta tehostetaan poikkeusoloissa rajoittamalla käyttövaltuuksia, tehostamalla käytönvalvontaa sekä eristämällä ja irrottamalla kriittisiä tietojärjestelmiä tai niiden osia verkoista.

7.10 Fyysinen turvallisuus

Keskeisten organisaatioiden keskuslaitteistot ja erityisesti operaattorien tietoliikennelaitteistot on pyrittävä jo normaalioloissa sijoittamaan vähintään väestönsuojaa vastaaviin tiloihin. Käyttöhenkilöstölle on varattava työskentelytilat näistä tiloista. Jos laitteistot eivät ole suojatiloissa, tilojen fyysisestä turvallisuudesta on huolehdittava muulla tavoin ja kohotettava valvontaa. Myös laitteiden suojaaminen, henkilöstön suojaan siirtyminen ja toiminnan jatkaminen on suunniteltava. Ainakin valtakunnallisesti tärkeiden laitteiden EMP-suojausta tulee harkita.

Pelastustoimilakiin perustuvan pelastustoimen tarkoituksena on tulipalojen ja muiden onnettomuuksien ehkäisy, ihmisten, omaisuuden ja ympäristön suojaaminen ja pelastaminen sekä väestönsuojelu. Yritykset, virastot ja laitokset ovat velvollisia omatoimisesti huolehtimaan pelastustoimenpiteistä ja laatimaan tätä varten suunnitelman.²⁴ Suunnitelmissa varaudutaan toiminnan turvaamiseen pelastustoiminnan keinoin. Yksityiskohtaisia ohjeita pelastustoiminnan suunnittelusta, valmisteluista ja toimeenpanosta antaa sisäasiainministeriö. Suunnitelmat on laadittava jo normaaliolojen varalle mutta niissä on otettava huomioon myös poikkeusolojen tarpeet. Poikkeusoloissa oman pelastustoiminnan merkitys korostuu viranomaisten sitoutuessa alueellisiin pelastustehtäviin.

7.11 Energian saanti

Poikkeusoloissa energian tuotantoon ja jakeluun kohdistuu olosuhteista riippuvia häiriöitä, jotka rajoittavat energiansaantia ja tekevät sen epäsäännölliseksi. Lisäksi viranomaisen valvoo ja säännöstelee energianjakelua ja -käyttöä. Tämän vuoksi poikkeusolojen energiansaanti vaatii suunnittelua ja valmistelua.

Erityistä huomiota tulee kiinnittää tietojärjestelmien ja tietoverkkojen sähkönsaantiin. Laitteiden tarvitseman sähkön saanti on varmistettava voimalaitteiden vikojen sekä sähköverkkojen jakeluhäiriöiden varalta. Varavoi-majärjestelmät mitoitetaan myös pitkäaikaisen käytön varalle.

Tuotannon valmiussuunnitelman yhteydessä laaditaan energiahuollon valmiussuunnitelma, joka sisältää kaikkien energiamuotojen tarpeet. Poik-

keusolojen tietotekniikan tarvitseman sähkön turvaaminen liitetään myös energiahuollon valmiussuunnitelmaan.

7.12 Toimintavaihtoehdot

Valmiuden kohottaminen

Poikkeusoloissa on välttämätöntä ryhtyä valmiuden vaatimiin toimenpiteisiin nopeasti ja joustavasti kohottamalla valmiutta.

Tietojenkäsittelyssä poikkeusolojen perusvalmius on olemassa, kun perusturvallisuus on toteutettu ja poikkeusolojen valmiussuunnitelma laadittu.

Perusvalmiudessa tulee suunnitelmasta olla toteutettuna ainakin seuraavat osat:

- turvallisuusorganisaatio (suunniteltu, nimetty ja koulutettu)
- henkilövaraukset
- varaosa- ja tarvikevarastointi
- normaaliolojen suunnitellut varalaitteet
- varatilojen käyttöönottosuunnitelma
- viestiyhteyksien varaamistoimenpiteet
- valmiussuunnitelman edellyttämät sopimukset
- sovellusten supistamissuunnitelma
- jäljelle jäävän tietojenkäsittelyn perustamissuunnitelma.

Kohotetussa valmiudessa on suoritettu ne valmiussuunnitelman toimenpiteet, joilla luodaan edellytykset toiminnan jatkamiselle poikkeusoloissa.

Kohotetun valmiuden saavuttamiseksi tulee suorittaa ainakin seuraavat toimenpiteet:

- tarkastetaan tietojenkäsittelyn valmiussuunnitelma turvattaviin toimintoihin ja tuotantoon liittyen
- toimeenpannaan varahenkilöjärjestelyt
- saatetaan varmistus- ja varajärjestelyt tarvittavine yhteyksineen toimintakuntoon
- alennetaan tietotekniikan käyttöastetta
- nopeutetaan välttämättömän materiaalin hankintoja ja
- tarkastetaan ja tehostetaan turvallisuusjärjestelyjä.

Täysvalmiudessa toiminta hoidetaan tarkistetun valmiussuunnitelman mukaisesti poikkeusolojen toimintana.

Kaikissa ulkomaankaupasta riippuvissa sopimuksissa on varauduttava sopimusten raukeamiseen syvissä kansainvälisissä kriiseissä (force majeure).

Tietotekniikan käyttöasteen alentaminen

Sovellusten purkamisjärjestys riippuu niiden merkityksestä ja sovellusten keskinäisestä sidonnaisuudesta. Purkamisjärjestys on yleensä sovellusten käänteinen tärkeysjärjestys. Sidosryhmät tulee ottaa huomioon sovelluksia purettaessa. Sovelluksilla tuotetaan ennen alasajoa ajan tasalla olevat lähökohdat manuaalitoimenpiteille tulostamalla esimerkiksi tietokantoja, varastotilanne ja tilauskanta sekä suojakopiot.

Tietotekniikan käyttöasteen alentaminen johtaa manuaaliseen toimintaan, johon tarvitaan lisätövoimaa. Sen hankkimiseksi otetaan yhteyttä työvoimaviranomaisiin. Työvoimaviranomaisten osoittaman työvoiman käyttö saattaa edellyttää kuljetuksien, majoituksen ja muun huollon järjestämistä. Mahdollista täydentävää työvoimaa organisaatiolle ovat sen omat eläkeläiset ja toimintaansa supistaneiden tietotekniikan palveluyritysten henkilöt, jotka tuntevat kyseisiä toimintoja.

Muuttuvat toiminnot, palvelutason lasku ja aikataulumuutokset edellyttävät tiedottamista sidosryhmille. Tietotekniikan käytön estyminen saattaa lopettaa toimintoja, jotka eivät ole mahdollisia ilman tietotekniikkaa. Näiltä osin toiminnan muutokset saattavat vaatia neuvotteluja eri sidosryhmien ja osapuolten, esimerkiksi tukku- ja vähittäiskauppojen, työnantaja- ja työntekijäjärjestöjen, Valtiokonttorin, Kansaneläkelaitoksen, vakuutuslaitosten ja pankkien kesken. Toimintasääntöjä joudutaan yksinkertaistamaan ja palvelutasoa laskemaan.

Tietotekniikasta luopuminen

Kauan jatkunut kriisi aiheuttaa tilanteen, jossa organisaation kaikkea tärkeätäkin tietojenkäsittelyä ei voida enää ylläpitää. Tietojenkäsittely ei esty yllättäen vaan se voidaan ennakoita tilannetta seuraamalla. Viranomaisten sääntely- ja säännöstelytoimenpiteiden vuoksi yhteiskunnan kannalta tärkeintä tietojenkäsittelyä voidaan ylläpitää vielä senkin jälkeen, kun joidenkin organisaatioiden tietojenkäsittely loppuu resurssipuutteiden vuoksi. Tietotekniikasta luopuminen tulee ennakoita siten, että elpyminen on mahdollista ja manuaaliset toiminnot ehditään käynnistää.

Todennäköisin syy tietotekniikan käytön rajoittumiseen ja loppumiseen on käyttöpalvelun, ohjelmistotuen ja varaosien puute. Pitämällä yhteyttä käytettävään huoltoyritykseen voidaan varaosien riittävyyttä seurata. Keskeisimmät tietotekniikan palveluyritykset ovat yleensä selvillä viranomaisten laatimasta huollettavien priorisoinnista, joten yllättävää huollon loppumista ei sääntelytoimenpiteiden johdosta tapahtune.

Sodanuhka ja sota johtavat organisaation käyttöön varattujen asevelvollisten kutsuntaan. Varamiesjärjestelyjen vaillinaisuus tai henkilöstön puute voivat aiheuttaa esteen tietotekniikan käytön jatkumiselle.

Tietotekniikasta luopumiseen voi johtaa myös perusrakenteiden ja ulkoisten palvelujen lamaan tuminen. Herkimpiä toimintoja ovat tietoliikenne ja energian jakelu. Myös toisen organisaation tietojenkäsittelyn estyminen voi johtaa oman tietojenkäsittelyn vaikeutumiseen.

Viranomaisten käynnistämä sääntely ja säännöstely voivat aiheuttaa manuaalisen varajärjestelmän käynnistämisen. Manuaalijärjestelmien on oltava toimivia varajärjestelmiä, jotka mahdollistavat nopean palaamisen tietotekniikan käyttöön.

7.13 Evakuointi ja siirtyminen

Vakavissa alueellisissa onnettomuuksissa ja poikkeusoloissa joudutaan väestö joskus siirtämään tilapäisesti turvalliselle alueelle. Tietojenkäsittelyä on varauduttava jatkamaan varsinaisissa tiloissa mahdollisimman kauan, sillä mahdollisuudet laitteistojen siirtoon ovat vähäiset. Henkilöstön evakuointi johtaa tietojentekniikan alasajoon ja suojaamiseen sekä tietoai-

neiston pelastamiseen. Poikkeusolojen uhatessa suojakopiot on toimitettava pois uhanalaisilta alueilta.

7.14 Elpyminen

Vaikka syvä kriisi olisikin pakottanut luopumaan tietotekniikasta, palataan sen käyttöön nopeasti kriisin mentyä. Tietotekniikkaa purettaessa on huomioitava tuleva elvyttäminen. Laitteistot, tiedostot ja tarvikkeet varastoidaan siten, että ne säilyvät käyttökelpoisina. Sovelluskohtaiset elpymissuunnitelmat on tehtävä ainakin tärkeimmille toiminnoille turvaamalla elpymisen vaatimat tiedot.

7.15 Testit ja valvonta

Valmiuden seurannan ja ylläpidon kannalta on tarpeen suorittaa valmiussuunnitelman tarkastus kerran vuodessa. Aika ajoin testauksen voi tehdä ns. pöytätestinä. Samalla on mahdollista täydentää suunnitelmat muutoksia vastaaviksi. Valmiusharjoituksessa testataan toipumissuunnitelman tai poikkeusolojen valmiussuunnitelman käyttöönotto.

Vähintään vuosittain tulee valmiudesta ja suunnitelmien ajantasaisuudesta raportoida myös organisaation ylimmälle johdolle.

7.16 Yhteistoiminta

Valmiussuunnittelussa tarvitaan yhteistyötä. Tärkeimpiä organisaation yhteistyötahoja tässä tarkoituksessa ovat palveluyritykset, tietotekniikan huoltoyritykset, verkko-operaattorit sekä eräissä tapauksissa myös media ja vaikeutuneissa olosuhteissa myös huoltovarmuudesta ja säännöstelystä vastaavat viranomaiset. Poikkeusoloissa tärkeät organisaatiot saavat täydentäviä ohjeita edellä mainituilta viranomaisilta.

Tietojenkäsittelyn poikkeusolojen valmiussuunnitelma (esimerkki)

Sisältö:

- Perusteet poikkeusolojen valmiudelle
 - valmiussuunnittelun tavoitteet
 - arvio poikkeusolojen vaikutuksesta toimintaan
 - valmiuden toteutusperiaatteet tietojenkäsittelyssä
- Toimivaltuudet
- Poikkeusolojen tuotantosuunnitelma
 - poikkeusoloissa ylläpidettävät toiminnot ja palvelut
 - sähköiset palvelut poikkeusoloissa
 - tietojärjestelmien tärkeysluokitus
 - riippuvuudet alihankkijoista
 - energian saannin varmistaminen
 - tarvikkeiden ja varaosien saanti/korvaaminen
 - toimintojen supistamissuunnitelmat ja uudelleen järjestelyt
- Poikkeusolojen tietojenkäsittelyn toteutus
 - toimintavaihtoehdot
 - valmiussuunnittelun vastuut, organisaatio poikkeusoloissa
 - tietojärjestelmien tärkeysluokitus poikkeusolojen kannalta
 - varmistettavat järjestelmät ja resurssit
 - laitteistokapasiteetin varaaminen
 - varaosien ja tarvikkeiden varaaminen
 - suojaus- ja pelastustoimenpiteet
 - varmuus- ja suojakopioiden säilytys ja käytön varmistaminen
 - henkilöstön käyttö poikkeusoloissa
 - henkilövarausten ylläpito ja henkilöstön koulutus
 - varatila- ja varakeskusjärjestelyt
 - valmiuden kohottaminen
 - siirtyminen täysvalmiuteen
- Energiansaannin turvaaminen
- Poikkeusolojen turvallisuustoimenpiteet ja suojele
 - fyysinen turvallisuus poikkeusoloissa
 - tietoaineiston turvallisuus
 - tietoturvallisuuden valvonta
- Tiedonsiirto
 - vaadittavat yhteydet, varmistettavat laitteet
 - vaihtoehtoiset tiedonsiirtotavat
- Tietotekniikan käytöstä luopuminen
 - keskittyminen kriittisiin järjestelmiin
 - korvaavat menettelyt ja laitteet
- Palaaminen normaalitoimintaan
 - elpymisedellytysten ylläpito
 - tekniset ja toiminnalliset edellytykset
- Tiedottaminen ja yhteydet
 - viranomaiset, alihankkijat
- Valmiuden ylläpito ja tarkastaminen
- Valmiustilanteen seuranta ja raportointi

8. TURVALLISUUS- JA VALMIUSSUUNNITTELUN TOTEUTUS

8.1 Käynnistysvastuu

Organisaation ylin johto vastaa valmiudesta sekä suunnittelun ja toimenpiteiden käynnistämisestä. Poikkeusolojen valmiussuunnittelun toteuttamiseksi tulisi yrityksissä nimetä käytännön toimenpiteistä vastaava ylemmän johdon alainen valmiuspäällikkö ja hänen avukseen tietotekniikan tunteva tietoturvallisuuspäällikkö. Valmiuspäällikön tehtävistä on esimerkki liitteessä 4a tietoturvallisuusvastuut ja tehtäväjako.

PTS:n poolit kouluttavat yhdessä HVK:n kanssa yritysten ja niiden toimipaikkojen nimettyjä valmiuspäälliköitä järjestämällä heille peruskoulutuksen sekä jatkokoulutusta tietyin aikavälein.

Muun turvallisuus- ja valmiushenkilöstön tarve määräytyy turvallisuustavoitteiden, organisaation laajuuden ja sen toimialan mukaan. Pienissä organisaatioissa voidaan yhdistellä tehtäviä ja hoitaa turvallisuustehtävät oman toimen ohella. Kun tietotekniikan käyttö on ratkaisevan tärkeää ja tietoturvallisuuden tarpeet suuret, turvallisuudesta ja valmiudesta vastaa päätoiminen turvallisuushenkilöstö.

8.2 Projektin organisointi

Parhaan lähtökohdan turvallisuuden ja valmiuden kehittämiseen antaa yrityksen avainhenkilöiden ja asiantuntijoiden laatima analyysi turvallisuudesta ja haavoittuvuudesta sekä sen perusteella tapahtuva turvallisuuden tason ja toimenpiteiden määrittely.

Tietoturvallisuuden kehittäminen on laajamittainen tehtävä. Työ on tarpeellista jakaa osakokonaisuuksiin kuten edellä on perusturvallisuudesta ja poikkeusolojen valmiudesta esitetty. Osahankkeille tulee nimetä vastuuhenkilöt. Vastuuhenkilönä voi olla valmiuspäällikkö apunaan tietotekniikan asiantuntija tai suunnittelu annetaan turvallisuusorganisaation tehtäväksi. Osahankkeille nimetään suunnitteluryhmä, jossa on edustettuna organisaation eri toiminnot. Ryhmään nimetään johdon edustaja, tärkeimpien käyttäjien edustajat, tietohallintojohtaja, käytön tekninen asiantuntija, valmiuspäällikkö, kiinteistöstä vastaava henkilö ja tietoturvallisuuden asiantuntija.

Suunnittelu voidaan suorittaa vaiheittain seuraavasti:

- asetetaan yrityksen toiminnan kannalta alustavat tavoitteet perusturvallisuudelle ja poikkeusolojen valmiudelle
- suoritetaan uhkien ja haavoittuvuuden analyysi ainakin tärkeimpien järjestelmien osalta
- määritellään elintärkeät järjestelmät
- tarkistetaan organisatoriset valmiudet turvallisuustoimenpiteisiin ja niiden kehittämistarpeet
- kootaan tiedot nykyisistä turvallisuustoimenpiteistä ja valmiuden nykytilasta sekä poikkeamat tarpeesta
- kootaan olemassa olevat suunnitelmat ja ohjeet

- kootaan fyysisen turvallisuuden toimenpiteet ja niiden nykytila sekä poikkeamat tarpeesta
- laaditaan toimenpidesuunnitelma perusturvallisuuden ja poikkeusolojen valmiuden kehittämiseksi
- laaditaan perusturvallisuuden suunnitelmat ja poikkeusolojen valmiussuunnitelma
- toteutetaan suunnitelmat.

Turvallisuus- ja valmiussuunnittelulla on oltava johdon tuki.

Hyväksymisen vaiheita ovat:

- tietoturvallisuuspolitiikka
- tavoitteet turvallisuudelle ja valmiudelle
- toteutusperiaatteet
- varajärjestelmäratkaisut ja -sopimukset
- koulutus ja informointi
- suunnitelmien vahvistaminen
- suunnitelmien toimeenpano
- investoinnit.

Jokaisella esimiehellä on organisaatiossaan vastuu myös turvallisuuden kehittamisestä, toteuttamisesta ja noudattamisesta.

8.3 Henkilöstön koulutus

Koko henkilöstön sitoutuminen turvallisuuteen on tärkeää varsinkin perusturvallisuudessa. Turvallisuuskoulutuksen tulee perustua organisaation omiin periaatteisiin, toteutustapaan ja ohjeisiin. Turvallisuussuunnittelu, toiminnan järjestäminen sekä johdon tietoturvallisuuspolitiikka ja päätökset antavat parhaimman perustan jatkuvalla omalle koulutukselle ja kehittämiselle hyväksytyjen tavoitteiden mukaisesti.

8.4 Valvonta

Suunnitelman laatiminen ei sellaisenaan riitä takaamaan valmiuden säilymistä. Perusehtona on laadittujen periaatteiden noudattaminen kaikessa tietojenkäsittelyn suunnittelussa, niin järjestelmien kehittämisessä kuin käytössäkin. Valmiuden pitäminen vaaditulla tasolla ja sen kehittäminen vaativat valvontaa. Valvonta on seuranta ja raportointia.

Turvallisuuden ja valmiuden kehittymisestä raportoidaan organisaation johdolle. Seurannasta vastaa tietohallintojohto, valmiuspäällikkö, turvallisuusorganisaatio, valmiusryhmä ja esimiehet omilla vastualueillaan.

Seurannan on kohdistuttava:

- ohjeiden noudattamiseen
- tietoturvallisuusrikkomuksiin ja niiden yrityksiin
- käyttötoimintoihin
- häiriöihin
- tietojärjestelmän haavoittuvuuden muutoksiin.

Organisaatiossa on seurattava sekä sisäisiä että ulkoisia riskitekijöitä. Vakavia riskejä on seurattava jatkuvasti johtoryhmässä.

Riskianalyysi on tarkistettava tarvittaessa ja uusittava vuosittain tai kun turvallisuustilanne tai tietotekniikka on muuttunut olennaisesti. Välittömiä muutostarpeita turvallisuussuunnitelmiin aiheuttavat yleensä laitteistomuutokset ja käyttötavan muutokset, hajauttaminen ja laajennukset, uudet verkko- ja tiedonsiirtoratkaisut, tietojenkäsittelyn ulkoistaminen ja tietotekniikkariippuvuuden muuttuminen sekä organisaatio- ja yritysmuutokset. Näihin liittyvien hankkeiden turvallisuus- ja valmiuskysymykset tulee ratkaista jo valmisteluvaiheessa.

Sisäinen seuranta kohdistuu jokapäiväiseen tietojenkäsittelyyn ja sen resursseihin. Olennaisimmat seurannan kohteet turvallisuuden kannalta ovat henkilöstön toiminta, käytön virheet ja häiriöt, luvattomuudet, haavoittuvuus, tietoturvallisuuden ja fyysisen turvallisuuden tilanne, sovellustyö, dokumentointi sekä kriisiorganisaation valmius.

Organisaation henkilöstön vaihtumista ja siirtoja toisiin tehtäviin on seurattava sekä henkilövarausten että sijaisuuksien vuoksi. Varatun henkilön sisäistä siirtoa ei tarvitse ilmoittaa sotilasläänin esikunnalle, ellei se vaikuta organisaation varauksiin. Sen sijaan esikunnalle on ilmoitettava henkilön varaustarpeen muutoksista ja varaustarpeen peruuntumisesta työsuhteen päättyessä.

9. YHDISTELMÄ

Yritysrakenteiden, tietotekniikan, organisaatioiden välisen verkottumisen sekä kansainvälisten yhteyksien ja palvelujen nopeiden muutosten vuoksi on organisaatioissa seurattava tiiviisti tietoturvallisuustarpeiden muutoksia. Tietoturvallisuuteen kohdistuvat paineet kasvavat.

Johdon on kiinnitettävä tietoturvallisuuteen huomiota enemmän ja tinki-mättömämmin kuin ennen. Verkkoriippuvuuden kasvaessa huomion tarve lisääntyy. Suuret riskit ja erityisesti hoitamattomat tai vaikeasti hoidettavat riskit on otettava jatkuvaan seurantaan. Johtoryhmän on huolehdittava tällaisesta määrämuotoisesta riskienseurannasta. Johdon on myös annettava varat tietoturvallisuusinvestointeihin ja niiden ylläpitoon.

Organisaation toiminnan jatkuvuuden varmistamisessa on viisainta varautua pahimman vaihtoehdon varalle selkein suunnitelmin. Esimerkiksi pörs-siyhtiössä yrityksen johto ottaa merkittävän riskin, ellei sillä ole suunnitel-maa erityistilanteisiin. Elintärkeät toiminnot on yksilöitävä ja määriteltävä niiden tärkeysjärjestys tietotekniikan varmistamiseksi, omistajien etujen turvaamiseksi erityistilanteissa ja yhteiskunnan toimivuuden ylläpitämiseksi poikkeusoloissa. Organisaation johdon tulee tietää, mitä tehdään ja mi-ten toimitaan keskeytystilanteissa ja poikkeusoloissa. Onko olemassa va-rajärjestelmiä tai jos niitä ei ole, milloin ne ovat valmiina. Usein niissä or-ganisaatioissa, joissa suunnitelmat on tekemättä, ei myöskään osata sanoa milloin ne tulevat kuntoon.

Erityisesti on huomattava, että

- ilman tietoturvallisuutta ei verkkoriippuvasta toiminnasta enää selvitä - on jouduttu tietoturvallisuusriippuvuuteen
- tietoturvallisuutta ei voida hallita ilman selkeitä peruslinjoja ja toiminta-an ja johtamiseen kytkettyjä suunnitelmia
- tietoturvallisuuden on oltava kunnossa, jotta kilpailukyky ja mahdolli-suudet uusiin palveluihin säilyvät
- asiakkaat ovat sitoutuneet jatkuvaan palvelujen saatavuuteen - tietojär-jestelmien toiminnan on oltava varmaa ja varajärjestelmin varmistettua
- turvallisuustoimenpiteet riippuvat enemmänkin palvelukykyvaatimuk-sista, tietojärjestelmärakenteista ja käyttötasosta kuin organisaation luonteesta
- tavoitteena on organisaation toiminnan jatkuvuus.

Johtamisen kannalta olennaista on tietoturvallisuustoimien oikea kohden-taminen. Yleisesti painopisteenä on ulkoisia verkkoja käyttävien tietojär-jestelmien tehokas suojaaminen hyökkäyksiltä ja itse tiedon suojaaminen salaamalla se tiedonsiirrossa ja verkoissa. Laajoissa verkottuneissa tietojär-jestelmissä on tärkeää huolehtia tietovarastojen eheydestä, käytettävyy-destä ja varmentamisesta. Luonnollisesti kansallisten ja yritys kohtaisten merkittävien tietokantojen suojaaminen on välttämätöntä. Menettelyinä ko-rostuvat luotettava, vahva todennus, salakirjoitus sekä sähköinen allekir-joitus, jotka on otettava nopeasti käyttöön.

Tietoturvallisuus tulee integroida toimintaan ja tietotekniikkaan. Turvalli-suustoimenpiteiden tulee muodostaa looginen ketju, jossa otetaan huomi-oon toimenpiteiden merkitys koko toiminnalle ja toisaalta varmistetaan,

etteivät ketjussa olevat puutteet vaaranna suojausarkkitehtuuria. Toimintaprosesseille asetettujen vaatimusten tulee peilata valmiuteen. Vanhoihin tietojärjestelmiin ja ohjelmistoihin ei ehkä pystytä rakentamaan niistä alunperinkin puuttuvia turvallisuusominaisuuksia. Saattaa olla, että vain pieni osa sovelluksista on sellaisia, joiden turvallisuusominaisuudet ovat vaadittavalla nykyaikaisella tasolla. Tällaiset puutteet on otettava erikseen käsitelyyn.

Kaikkien tietotekniikasta riippuvien organisaatioiden on varauduttava tietoteknisiin erityistilanteisiin, jollaisiin voidaan joutua hyvinkin nopeasti tietoteknisten vaurioiden tai perusjärjestelmien vahingoittamisen seurauksena.

Tietoturvallisuudella on yhä tärkeämpi merkitys yhteiskunnan poikkeusolojen valmiudessa. Toimintaedellytykset riippuvat ratkaisevasti tärkeiden organisaatioiden tietotekniikan poikkeusolojen valmiudesta. Sellainenkin organisaatio, jolla ei ole valmiusvaatimuksia, tarvitsee suunnitelman tietovarastojen suojaamisesta normaaliin toimintaan palaamiseksi.

Laajojen tietojärjestelmien varmistaminen vaatii toimenpiteitä kaikilta tietojenkäsittelyn osapuolilta, yrityksiltä, julkisyhteisöiltä, verkkojen ylläpitäjiltä ja tietotekniikan palveluyrityksiltä.

VIITTEET

LIITE 1

- 1 Valmiuslaki 22.7.1991/1080, muutos 198/2000
- 2 Laki huoltovarmuuden turvaamisesta 18.12.1992/1390
- 3 Huoltovarmuuden tavoitteiden tarkistaminen, KTM:n työryhmä- ja toimikuntaraportteja 12/2001
- 4 Telemarkkinalaki 396/1997, muutokset 596/1998, 139/1999, 566/1999, 314/2001, 893/2001, 1119/2001
- 5 Laki puolustustaloudellisesta suunnittelukunnasta 20.5.1960/238, muutokset 1241/1987, 623/1999
- 6 Asetus puolustustaloudellisesta suunnittelukunnasta 20.5.1960/239, muutokset 42/1981, 1391/1992
- 7 Asetus valtionhallinnon tietohallinnosta 12.2.1988/155, muutos 1401/1992
- 8 Valtioneuvoston periaatepäätös valtionhallinnon tietohallinnon kehittämisestä, VM 2.3.2000 (VM0087:00/00/02/02/1999)
- 9 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta, VM 11.11.1999/0024:00/02/99/1988
- 10 Selvitys Internetin turvallisuusriskeistä, PTS Sähkö- ja elektroniikka-pooli
- 11 Laki yksityisyyden suojasta työelämässä 477/8.6.2001
- 12 Laki viranomaisen toiminnan julkisuudesta 21.5.1999/621
- 13 Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030
- 14 Valtionhallinnon tietoaineiston käsittelyn tietoturvallisuusohje (VAHTI 2/2000, Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje (VM 5/01/2000)
- 15 Henkilötietolaki 22.4.1999/523
- 16 Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta 22.4.99/ 565/1999, muutokset 532/2000, 1148/2001
- 17 Asetus yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta 22.4.99/ 723/1999
- 18 Internetin käyttöön liittyvät uhat ja niihin varautuminen, PTS Tietojärjestelmäjaoston julkaisu 2/2000
- 19 Arkistolaki 23.9.1994, 831/94
- 20 Arkistolaitoksen ohje arkistolain piiriin kuuluvien sähköisten tietojärjestelmien ja tietoaineistojen käsittelystä, Arkistolaitos määräys 22.5.2001, ohje 126 /40/01
- 21 Turvavarastolaki 17.12.1982/970, KTM:n päätös yritysten turvavarastointiin myönnettävien korkotukilainojen yleisistä ehdoista 12.5.1993
- 22 Asetus vapauttamisesta asevelvollisuuden suorittamisesta eräissä tapauksissa 22.11.1968/653
- 23 Atk-avainhenkilöstön varaaminen 13.9.1993, PTS 5301/93
- 24 Pelastustoimilaki 30.4.1999/561 ja pelastustoimiasetus 27.8.1999/857

Eheys

Tiedot ja järjestelmät ovat aitoja, ristiriidattomia, oikeellisia, luotettavia, kattavia, ajantasaaisia ja käyttökelpoisia, eivätkä ne ole hallitsemattomasti tai valtuudettomasti muuttuneet, mahdolliset muutokset voidaan todeta kirjausketjusta.

Elektromagneettinen pulssi (EMP)

EMP on ydinräjähdyksessä syntyvä voimakas ja nopea elektromagneettinen pulssi, joka tuhoaa suojaamattomat elektroniset komponentit.

Elintärkeä järjestelmä tai sovellus

Järjestelmän omistajan määrittelemä järjestelmä tai sovellus, joka on välttämätön elintärkeiden toimintojen ylläpitämiseksi.

Erityistilanteet

Erityistilanteilla tarkoitetaan normaaliolojen vakavista häiriöistä mm. tietotekniikka- ja verkkoriippuvuudesta aiheutuvia olosuhteita, joissa tietotekniikan käytön varmistamiseen on varauduttava joiltakin osin poikkeusolojen tavoin.

Etähallinta

Etähallinnalla tarkoitetaan tietojärjestelmän käyttötoiminnan - järjestelmän hallinnan ja operoinnin - tai jonkin järjestelmäosuuden käyttötoimenpiteiden tai ylläpidon hoitamista oman lähiverkon ulkopuolelta.

Etätyö

Etätyöllä tarkoitetaan tietoverkkoon kytketyllä työasemalla säännöllisesti muualla kuin vakituisella työpaikalla tehtävää työtä ollen jatkuvassa tai säännöllisessä yhteydessä työpaikkaan.

Etäyhteys

Yhteys organisaation lähiverkkoon ja sen palveluihin organisaation tilojen ulkopuolelta matkalla tai etätyön vuoksi.

Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan laitteiden, aineistojen, varastojen ja toimitilojen suojaamista tuhoja ja vahinkoja vastaan sekä ympärysjärjestelmien, kuten sähkösyötön varmistamista.

Hallinnollinen tietoturvaluisuus

Hallinnollisella tietoturvaluudella tarkoitetaan tietoturvaluisuuden toimintalinjojen periaatteiden, turvallisuustoiminnan organisaatiojärjestelyjen, henkilöstön tehtävien ja vastuiden määrittelyn sekä tietoturvaluisuusohjeiston, koulutuksen ja valvonnan muodostamaa kokonaisuutta.

Henkilörekisteri

Henkilörekisterillä tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa tietojoukkoa, joka sisältää kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi ja jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta.

Henkilöstöturvaluisuus

Henkilöstöturvaluudella tarkoitetaan henkilöstön luotettavuuteen ja soveltavuuteen, toimenkuvien, sijaisuuksien, tiedon saanti- ja käyttöoikeuksien, henkilöstön suojaamisen, koulutuksen ja valvonnan muodostamaa kokonaisuutta.

HPM-ase (High Power Microwave)

HPM-ase on radiotaajuudella tutkan kaltaisesti lähettävä sähköinen ase, joka aiheuttaa kohteena olevien elektronisten järjestelmien ympärille vaarallisen elektromagneettisen kentän vaurioittaen moderneja mikroprosessoreja ja häiriten niiden toimintaa. Kohteessa ei kenttää voida havaita ilman ilmaisimia.

Huolto- ja laitevalmiussopimus

Sopimus määrittelee ennalta toimitusajan, jonka kuluessa tuhon jälkeen huolletut laitteistot ovat normaalikäytössä.

Huoltovarmuus

Huoltovarmuudella tarkoitetaan väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömien taloudellisten toimintojen turvaamista poikkeusolojen varalta.

Kiistämättömyys

Varmistaa sähköisesti, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys) tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi.

Käytettävyys

Tieto, tietojärjestelmä tai palvelu ovat niihin oikeutettujen saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvää kokonaisuutta.

Laitteistoturvallisuus

Laitteistoturvallisuus käsittää tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyden, toiminnan, kokoonpanon, kunnossapidon ja laadunvarmistuksen.

Luottamuksellisuus

Tiedot ja järjestelmät ovat vain niiden käyttöön oikeutettujen käytettävissä, sivullisille ei anneta mahdollisuutta muuttaa tai tuhota tietoja eikä muutoin käsitellä tietoja.

Normaaliolot

Normaalioloilla tarkoitetaan tavanomaisia oloja ja organisaation tavanomaista toimintaa.

Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmien, väli-, sovellus- ja tietoliikenneohjelmistojen turvallisuusominaisuuksia, kuten tunnistamis-, eristämisen-, pääsynvalvonta- ja varmistamismenettelyjä, havainnointi- ja paljastusmenetelmiä, lokimenettelyjä, turvallisuussovelluksia sekä näiden laadunvarmistuksen, ylläpidon ja päivityksen muodostamaa kokonaisuutta.

Palomuuriratkaisu

Turvapalvelimella toteutettu verkot yhdistävä rajapinta, joka päästää lävitseen vain valtuutetut käyttäjät tai sallitun tietoliikenteen.

Perusturvallisuus

Perusturvallisuudella tarkoitetaan tietoturvallisuuden tilaa, joka perustuu tietoturvallisuussuunnitelmaan ja toipumissuunnitelmaan ja jossa organisaatio on varautunut normaalioloissa tapahtuviin vahinkoihin ja keskeytyksiin.

Poikkeusolot

Poikkeusoloilla tarkoitetaan tässä yhteydessä valmiuslaissa määriteltyjä poikkeusoloja.

Poikkeusolojen valmiussuunnitelma

Poikkeusolojen valmiussuunnitelma määrittelee tietojenkäsittelyn tasovaatimukset poikkeusolojen varalle, palvelujen hallitun supistamisen ja elpymistoimenpiteet normaalioloihin palaamiseksi. Poikkeusolojen valmiussuunnitelmalla organisaatio on varautunut poikkeusoloissa syntyviin ongelmiin, vahinkoihin ja keskeytyksiin.

Sähköinen allekirjoitus

Sähköisellä allekirjoituksella tarkoitetaan tietojoukkoa, joka varmistaa sähköisen viestin alkuperän ja eheyden julkisesti tarkistettavan menetelmän avulla.

Suojakopio

Tietokantojen ja sovellusten kopiot, jotka ovat välttämättömiä elintärkeiden järjestelmien toipumiselle. Suojakopiot säilytetään toisessa kiinteistössä mahdollisesti eri paikakunnalla. Suojakopioiden tulee mahdollistaa vakavankin tuhon jälkeen toipuminen ja tietojenkäsittelyn käynnistäminen uudelleen.

Suojausarkkitehtuuri

Suojausarkkitehtuurilla tarkoitetaan tietojärjestelmien systemaattisten turvallisuusmenettelyjen kokonaisuutta tietojenkäsittely-ympäristössä ja -prosessissa.

Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden turvaamista mm. tietoaineiston luettelointi- ja luokitusmenettelyin sekä tietoaineiston asianmukaisella hallinnalla, käsittelyllä, säilytyksellä ja hävittämisellä.

Tietojärjestelmän omistaja

Tietojärjestelmän omistaja on se nimetty taho, jota järjestelmä ensisijaisesti palvelee ja joka myös vastaa järjestelmän tietojen turvallisuudesta ja toimintavarmuudesta oman toiminnan sekä tietojärjestelmästä riippuvien muiden toimintojen varmistamiseksi.

Tietojenkäsittely

Tietojenkäsittelyllä tarkoitetaan kaikenlaista tietojen käsittelyä manuaalisesti tai tietotekniikkaa toiminnoissa hyödyntäen.

Tietojenkäsittelyn turvallisuussuunnittelu

Tietojenkäsittelyn turvallisuussuunnittelulla tarkoitetaan turvallisuusanalyysin, perusturvallisuuden suunnittelun, poikkeusolojen valmiussuunnittelun ja turvallisuustoimenpiteiden muodostamaa suunnitteluprosessia.

Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan tietoliikennelaitteiston kokoonpanon, sen luetteloinnin, ylläpidon ja muutosten valvonnan, ongelmatilanteiden kirjauksen, käytön valvonnan, verkon hallinnan ja pääsynvalvonnan, viestinnän salauksen, verkon varmistamisen, tietoturvallisuuden kannalta merkityksellisten tapahtumien tarkkailun, kirjauksen ja selvittämisen sekä tietoliikenneohjelmien testauksen ja hyväksymisen muodostamaa kokonaisuutta.

Tietotekniikan turvallisuus

Tietotekniikan turvallisuus käsittää tietotekniikkaan, kuten tietoliikenteeseen, laitteistoihin, ohjelmistoihin ja niiden käyttötoimintaan kohdistuvat turvallisuustoimenpiteet ja niiden ylläpidon.

Tietotekniikan varmistaminen

Tietotekniikan varmistaminen käsittää turvallisuustoimenpiteet, joilla toiminta turvataan myös vakavissa vahinkotilanteissa varsinaisen tietotekniikan käytön estyessä. Tietotekniikan varmistaminen voi tapahtua omin varalaitteistoin tai käyttäen varakeskuksia.

Tietoturvaluuspolitiikka

Valtion tasolla tietoturvaluusnormien ja niiden täytäntöönpanon muodostama kokonaisuus. Organisaation tasolla johdon hyväksymä näkemys tietoturvaluuden päämääristä, periaatteista ja toteutuksesta.

Tietoturvaluussuunnitelma

Tietoturvaluussuunnitelma määrittelee elintärkeät tietojärjestelmät sekä periaatteet ja vaatimukset perusturvaluudelle ja poikkeusolojen valmiudelle tiedon ja tiedonsiirron suojausten, laitteistojen ja ohjelmistojen turvaluuden ja tietojärjestelmien fyysisen suojan kehittämiseksi ja ylläpitämiseksi sekä tarvittavan materiaalin turvaamiseksi.

Todennus

Tietojärjestelmän käyttäjän tai viestinnässä toisen osapuolen luotettava sähköinen tunnistaminen.

Toipumissuunnitelma

Toipumissuunnitelma määrittelee elintärkeille tietojärjestelmille suurimmat sallitut keskeytysajat, varajärjestelmäsopimukset, huollolle asetettavat vaatimukset, varajärjestelmiin siirtymisajat ja toipumisaikavaatimukset, vastuut ja toimenpiteet valmiuden luomiseksi sekä valmiuden ylläpidon vaatimat testaukset, seurannan, raportoinnin, toimeenpanon ja palaamisen normaalitoimintaan sekä ohjeet toiminnasta erilaisissa keskeytys ja erityistilanteissa.

Toipumissuunnitelman testaus

Testissä kokeillaan elintärkeän järjestelmän toipuminen kuvatuissa katastrofitilanteissa.

Turvaluusmäärittely (tietoturvaluus)

Turvaluusmäärittelyllä tarkoitetaan organisaation toimintojen tarpeista lähtevää, tietojenkäsittely-ympäristön - henkilöstön, käyttöympäristön, kytkentäympäristön ja laitekannan - sekä tietotekniikkariippuvuudet huomioon ottavaa turvaluusmenettelyjen määrittelyä.

Valmiusraportti

Järjestelmän omistajan vuosittainen raportti valmiudesta ylläpitää elintärkeät tietojärjestelmät.

Valmiustarkastus

Valmiustarkastuksella tarkastetaan vuosittain edellä esitettyjen suunnitelmien ajantasaisuus, varajärjestelmäsopimusten voimassaolo, varmuus- ja suojakopioiden säilytys ja käytettävyyys sekä varmistetaan testien ja muiden toimenpiteiden suorittaminen.

Varakeskus

Toimintaan valmisteltu, testattu ja sopimuksin valmisteltu tietokonekeskus.

Varakonesopimus

Sopimus, joka toipumissuunnitelman osana varmistaa kriittisten sovellusten käytön, tarvittavan koneajan saannin sekä mahdollisuudet testausten suorittamiseen.

Varatila

Ennalta valmisteltu toimitila, jossa tuhon sattuessa toimintaa voidaan jatkaa.

Varmuuskopio

Tiedostot ja sovellukset, joiden kopioita käytetään normaalitilanteissa tiedostojen palauttamiseen. Varmuuskopiot säilytetään välittömän käytön varalle fyysisesti suojattuina käyttökohteessa.

Muut käsitteet

Laajemmin tietoturvaluuden käsitteet on esitetty ohjeessa Valtionhallinnon tietoturvaluuskäsitteistö, VAHTI 1/2000.

Valtiovarainministeriö/Valtionhallinto

- Toimet tietoturvaluusloukkaustilanteissa, Vahti 7/2001
- Valtion tietotekniikkahankintojen tietoturvaluuden tarkistuslista, Vahti 6/2001
- Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje, Vahti 5/2001
- Sähköisten palveluiden ja asioinnin tietoturvaluuden yleisohje, Vahti 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvaluussuositus, Vahti 3/2001
- Valtionhallinnon lähiverkkojen tietoturvaluussuositus, Vahti 2/2001
- Valtion viranomaisen tietoturvaluustyön yleisohje, Vahti 1/2001
- Tietokoneviruksista ja muilta haittaohjelmilta suojautumisen yleisohje, Vahti 4/2000
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvaluussuoritus, Vahti 3/2000
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvaluusohje, Vahti 2/2000
- Valtionhallinnon tietoturvaluuskäsitteistö, Vahti 1/2000
- Tarpeettomaksi tulleiden tietoaineistojen hävittäminen, VM 21/01/2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 5/01/2000
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvaluussuositus, Vahti 2/1999
- Valtion etätyön tietoturvaluussuositus, Vahti 1/1999
- Suositus toimilaturvaluuden huomioonottamisesta valtionhallinnossa, VM 30.12.1998
- Valtion Internetin käyttö- ja tietoturvaluussuositus, Vahti 1/1998
- Tietoturvaluuden tulosohjaus ja kehittämisvälineet, Vahti 2/1997

Päivitykset:

<http://www.vn.fi/vm/kehittaminen/tietoturvaluus/vahti/vahti2.htm>

Puolustustaloudellinen suunnittelukunta/Huoltovarmuuskeskus

- Internet, toiminnan verkottuminen ja sen haavoittuvuus, PTS 2001
- Raportti tietojärjestelmäalan kriisivalmiudesta, PTS 2001
- Tiedonsiirron muutos- ja uhka-analyysi, PTS 2001
- Tiedonsiirron ja -käsittelyn muutos- ja uhka-analyysi, PTS 2001

Päivitykset:

<http://www.nesa.fi>

Sähköinen säädöskokoelma:

<http://www.finlex.fi>

TIETOTURVALLISUUSVASTUUT JA TEHTÄVÄJAKO

Organisaation ylimmän johdon tehtävät:

- määrittellä ja vahvistaa tietoturvallisuuspolitiikka
- vahvistaa turvallisuustoiminnan periaatteet ja palvelusvaatimukset
- velvoittaa yksiköiden/toimintojen johto tunnistamaan riskit ja määrittelemään elintärkeät sovellukset
- tuntea tietoturvallisuuden taso ja valmius keskeytyksiin
- luoda edellytykset suunnittelulle ja toteutukselle
- määrittellä poikkeusoloissa ylläpidettävät toiminnot
- järjestää isojen riskien jatkuva määrämuotoinen seuranta johtoryhmässä.

Yksikön, toimipaikan ja toiminnon johdon tehtävät:

- nimetä järjestelmien omistajat ja määrittellä heidän vastuunsa turvallisuudessa
- varmistaa, että järjestelmien omistajat ovat asettaneet elintärkeille toiminnoille ja niitä tukeville tietojärjestelmille turvallisuusvaatimukset
- tarkistaa vuosittain valmius turvallisuuden ylläpitämiseen, toipumiseen ja erityis-tilanteisiin
- raportoida vuosittain johdolle elintärkeiden järjestelmien turvallisuuden ja valmiuden muutokset.

Tietojärjestelmän omistajan tehtävät:

- perusturvallisuuden toimeenpano, toipumisvalmius ja valmiussuunnittelu
- suunnitelmien päivittäminen vuosittain
- varmuuskopioinnin ja suojakopioinnin tarkastaminen
- raportointi tietohallintojohdolle vuosittain muutoksista sekä kyvystä varmistaa toiminta.

Tietohallintojohdon tehtävät:

- määrittellä tietojärjestelmille tekniset turvallisuustavoitteet
- tarkistaa, että organisaation elintärkeiden järjestelmien varmistamiseen on suunnitelmat ja ne säilytetään toimintatilojen ulkopuolella
- määrittellä periaatteet ulkoistettujen palvelujen käytössä noudatettavalle tietoturvallisuudelle, toipumiselle ja poikkeusolojen valmiudelle
- varmistaa, että henkilökunta on koulutettu turvallisuustoimenpiteisiin
- varmistaa, että suunnitelmat päivitetään vuosittain
- koota organisaation elintärkeiden järjestelmien tiedot ja
- raportoida valmiudesta ja esittää arvio suunnitelmien laadusta johdolle vuosittain.

Tietoturvallisuusvastuuhenkilön tehtävänä on:

- osallistua tietoturvallisuuspolitiikan ja -periaatteiden määrittelyyn
- avustaa johtoa ja yksiköitä tietoturvallisuuden toimeenpanossa
- kehittää tietoturvallisuutta turvallisuuspolitiikan mukaisesti
- huolehtia henkilöstön turvallisuustietoisuuden lisäämisestä ja tietoturvallisuuskoulutuksen järjestelystä
- ohjata tietoturvallisuuden käytännön toteutusta ja siihen liittyvää riskienhallintaa
- järjestää tietoturvallisuutta koskeva seuranta ja johdon informaatio ja kehittää ehdotuksin tietoturvallisuutta
- raportoida ylimmälle johdolle tietoturvallisuudesta.

Tuotantojohdon tehtävät:

- määrittellä tuotannon tietojärjestelmille perusturvallisuuden turvallisuustavoitteet
- määrittellä poikkeusolojen tuotannon tietojärjestelmille turvallisuus- ja valmiustavoitteet
- tarkistaa, että tuotannon elintärkeiden järjestelmien varmistamiseen on suunnitelmat ja tarvittavat suojakopiot ja ne säilytetään toimintatilojen ulkopuolella
- varmistaa, että henkilökunta on koulutettu turvallisuustoimenpiteisiin
- varmistaa, että suunnitelmat päivitetään vuosittain
- raportoida valmiudesta ja esittää arvio suunnitelmien laadusta ylimmälle johdolle vuosittain.

Sisäisen tarkastuksen tehtävät:

- arvioida tietoturvallisuuden tasoa organisaation riskienhallinnan kannalta
- valvoa tietoturvallisuuden toteutumista lain, säädösten ja määräysten edellyttämällä tasolla sekä toiminnan tärkeyden ja laadun huomioon ottaen
- valvoa erityisesti elintärkeiksi määriteltyjen järjestelmien turvallisuutta koskevien johdon määrittelemien vaatimusten toteutumista.

Valmiuspäällikön tehtävät:

- organisaation valmiussuunnittelun koordinointi, toteuttaminen ja ajan tasalla pitäminen
- valmiustekijöiden seuranta
- tuotannon valmiussuunnitelman laatiminen ja ylläpito
- tietotekniikan poikkeusolojen valmiusvaatimusten määrittely tietojenkäsittelyn poikkeusolojen valmiussuunnitelman laatimiseksi
- toiminnan kannalta kriittisten materiaalien varastotilanteen seuranta
- tuotannon muutosvalmiuden selvittäminen
- korvaavan tuotannon selvittäminen
- korjaus- ja huoltotoiminnan varmistaminen
- energiansaannin varmistaminen ja vaihtoehtoisten energialähteiden selvittäminen
- kuljetusvaraukset
- VAP-varaukset
- työvoiman uudelleenjärjestely, koulutustarpeen selvittäminen, lisätyövoiman hankinta
- valmiussuunnitelman tarkastus ja testaus
- seurannan perusteella edellä olevien toimien parannusesitykset johdolle
- valmiuskoulutuksen järjestäminen.

Tarkastuslista on tarkoitettu tietoturvallisuuden, toipumisvalmiuden ja poikkeusolojen uhkien arviointiin.

Normaaliin käyttöön kohdistuvat uhat

- virheet ohjelmistoissa ja käyttövirheet
- laitteiden rikkoutuminen, ympäristön vaikutukset: lentoliikenne, räjäytykset, raskas liikenne, rakennustyöt
- lähiverkon häiriöt, tietoliikenneyhteyksien häiriöt, virransyötön keskeytyminen ja jakeluhäiriöt
- epäluotettava henkilöstö ja ristiriidat työsuhteissa, lakko
- tehtävien keskittyminen ja avainhenkilöriippuvuus
- henkilöstön saneeraukset ja ylikuormitus
- tietovuodot, tietojen anastaminen, muuttaminen, vahingoittaminen ja tuhoaminen verkoissa
- tietokonevirukset
- väärin tietojen syöttäminen, tekaistujen tilauksien teko ja tietokantojen, toimitus- ja hintatietojen sekä Internet-sivujen muuttaminen
- ulkopuolelta häiriöiden tuottaminen ja muuten toimintaan ja palveluihin vaikuttaminen
- palvelujen ulkoistamisen seurauksena tietojen luvaton käyttö ja haitanteko, hallitseman riippuvuus tietojenkäsittelypalveluista sekä etähuoltoyhteyksien ja järjestelmien etähallinnan valtuuksien väärinkäyttö
- tietokantoihin tunkeutuminen kotimaisista ja kansainvälisistä verkoista, haittaohjelmien toimittaminen järjestelmiin, verkon kautta tapahtuva sabotaasi, vahingonteko ja ilki-valta
- kilpailuetuja antavien tietojen vakoilu ja anastus sekä
- tietoliikenneyhteyksien ja verkkojen käytön häirintä.

Toiminnan jatkuvuuteen kohdistuvat uhat

- perusturvallisuuden puutteet ja niiden seurauksena syntyvät viat, virheet, rikkoutumiset ja luvattomuudet
- ohjelmavirheet ja ohjelmistoille aiheutuvat tuhot vikatilanteissa ja laitteiden tuhoutessa tai muista ulkoisista häiriöistä
- tietojärjestelmän osissa sattuvat vakavat häiriöt
- tukipalvelujen häiriöt, palveluyritysten henkilöstö-, organisaatio- ja omistajuusmuutokset
- tietoliikenneyhteyksien tuhoutuminen
- konesali-, palvelin- ja tietoliikennetilojen ja -laitteiden tuhoutuminen fyysisten vahinkojen ja onnettomuuksien, kuten vesivuoto-, tulva-, pohjavesi-, tulipalo-, savu-, sammutus-, ukkos-, sortuma- ja lämpövahinkojen seurauksena
- keskeisiin tietojärjestelmiin tunkeutuminen ja sabotointi sekä tietojärjestelmien toiminnan lamauttaminen
- sähkösaannin häiriöt
- vakaviin keskeytyksiin johtavat haittaohjelmat ja virukset
- palvelutoimittajille ja verkko-operaattoreille sattuvat vastaavat tapahtumat
- painostusryhmien haitanteko
- terrori
- informaatioodankäynti tai sen valmistelu.

Eriytilanteet

- tietotekniikkaa tukevien perusjärjestelmien (sähkö, verkot) tuhoutuminen
- paikallinen tai alueellinen onnettomuus ulkomailla aiheuttaen tärkeiden kansainvälisten tietoliikenneyhteyksien katkeamisen sekä organisaation toiminnan ja tietojärjestelmien vakavan keskeytymisen

- terrori, jonka seurauksena tietoliikenneyhteydet katkeavat tai katkaistaan
- tarkoituksellinen kansainvälisten tietoliikenneyhteyksien katkaisu turvallisuustoimenpiteenä.

Poikkeusolojen tietojenkäsittelyyn kohdistuvat uhat

- vakavat ja pitkäaikaiset fyysiset tuhot ja tietoverkkojen ja kriittisten osajärjestelmien käytön estyminen suuronnettomuuden, ydinonnettomuuden tai terrorismin seurauksena
- jakeluverkkojen häiriöt ja tuhot, energian tuotannon tai jakelun häiriöt ja säännöstely sekä käytön pitkäaikaiset katkot, yleinen energiapula ja kuljetushäiriöt
- tietoliikenteen häiriöt ja keskeytykset, tarkoituksellinen yhteyksien katkaisu tai vaurioituminen, maailmanlaajuisten verkkojen käytön estyminen ja käytön säännöstely
- ulkomaisten palvelujen rajoittuminen tai loppuminen: palvelukeskus-, etähuolto-, erikoisasiantuntija- ja tukipalvelujen kaventuminen
- avainhenkilöriskien korostuminen, avainhenkilöiden menetys, yleinen työvoimapula, epidemia, kutsunnat
- laitteistojen käytettävyyden heikkeneminen pitkään jatkuvassa kauppasaarrossa, tuontiin sidottujen tietojenkäsittelylaitteiden varaosien ja tietoteknisten tarvikkeiden saannin vaikeutuminen tai estyminen
- haitan- ja vahingontekojen lisääntyminen
- fyysisten vahinkojen toistuminen, fyysisten turvallisuustoimenpiteiden tärkeyden korostuminen
- ohjelmistoille ja komponenteille vahinkoja aiheuttavat voimakkaat sähkömagneettiset häiriöt, elektromagneettinen pulssi (EMP) ja elektronisen sodankäynnin aseet (HPM)
- omaan toimintaan käytettävän laitekapasiteetin väheneminen viranomaisten säännöstellässä tietotekniikan käyttöä tai ohjatessa laitteistoille muita töitä
- tietosodankäyntiin liittyvä tahallinen häirintä ja sabotointi, tietojärjestelmiin tunkeutuminen, tietojenkäsittelyn tahallinen sabotointi, haittaohjelmien toimittaminen järjestelmiin, kansallisten tietokantojen tuhoaminen tai anastaminen ja tietoliikenneyhteyksien katkaisu
- poliittisten ja sotilaallisten tahojen sekä erilaisten yhdenasianliikkeiden ja järjestäytyneen rikollisuuden suorittama tietojärjestelmiin tunkeutuminen
- ulkopuolisten tahojen suorittama kriittisten materiaalitoimitusten häirintä ja estäminen
- suojautumisen ja väestön evakuoinnin aiheuttamat toiminnan keskeytykset
- sodan tuhojen seurauksena keskeisimpien perusrakenteiden ja laitteistojen tuhoutuminen.

HAAVOITTUVUUDEN JA VALMIUDEN ARVIOINTI LIITE 4c

Tarkastuslista on tarkoitettu tietoturvallisuuden, toipumisvalmiuden ja poikkeusolojen haavoittuvuuden ja valmiuden arvioinnin apuvälineeksi.

Tietoturvallisuuden arviointi

- suoritetaan toimintojen ja palvelujen turvallisuustarpeiden arviointi eheyden, luottamuksellisuuden, käytettävyyden, todentamisen ja kiistämättömyyden kannalta
- tarkastelu ulotetaan organisaation koko tuotantoon, palveluihin, tietoverkkoihin, tietoliikenteeseen, tietojenkäsittelyyn, hallintoon, henkilöstöön, fyysiseen suojaan, laitteistoihin, ohjelmistoihin, tietoaineistoon ja käyttötoimintaan
- otetaan huomioon organisaation riippuvuudet omista tietojärjestelmistä, verkoista ja käytetyistä tietojenkäsittelypalveluista, muut ulkoiset riippuvuudet sekä muiden riippuvuudet omista palveluista
- määritellään elintärkeät järjestelmät, joissa tietotekniikkariippuvuus on suuri
- arvioidaan tietoriskit, keskeytysriskit ja henkilöriskit
- kohdistetaan tarkastelu päätoimintoihin ja niille asetettuihin palvelujen ja toiminnan vaatimuksiin arvioiden riskien vaikutukset ja todennäköisyydet
- valitaan joukko riskitilanteita ja kuvataan ne sekä niiden vaikutukset valituissa järjestelmissä, riskin syntymiseen vaikuttavat tekijät, vahingon suuruus ja todennäköisyys
- tietotekniikkariippuvuuden taso
- tietoturvallisuusohjeiden noudattaminen
- tapahtumien havainnointimenettelyt
- käyttöoikeuksien, käytön ja verkon valvonta
- yhteensopivuus
- järjestelmäkehitys ja testaus
- tietojenkäsittelyn fyysinen turvallisuus ja valvonta
- verrataan olemassa olevat menettelyt todettuihin tarpeisiin
- selvitetään turvallisuustoimenpiteiden tärkeysjärjestys
- tuotetaan toimenpide-ehdotukset ja toteutussuunnitelma.

Toipumisvalmiuden arviointi

- yhteiskäyttöketjussa olevien tietojärjestelmien keskinäiset riippuvuudet
- tietokantojen, sovellusten ja koko tietojenkäsittelyn eheyden säilyttäminen ja käytettävyys hallitsemattomissa keskeytyksissä
- keskitettyjen, koko verkolle välttämättömien tietojenkäsittelyresurssien ylläpito (verko-ko aika, nimipalvelu ja hakemistopalvelu)
- tietojenkäsittelylle kriittisten verkon laitteiden varmistaminen (viat, sähkökatkot)
- verkkojen hallinta keskeytystilanteessa
- riippuvuus ulkopuolisista palvelutuottajista
- alueellisista, valtakunnallisista ja maailmanlaajuisista osuuksista rakentuva tietojenkäsittely.

Tietojenkäsittelyn poikkeusolojen valmiuden arviointi

- tietotekniikan merkitys organisaatiolle ja asiakkaille poikkeusoloissa
- organisaation toiminnan, tuotannon tai palvelun merkitys kansalaisten ja yhteiskunnan toimeentulolle eri tilanteissa
- valtiovallan asettamat poikkeusolojen tuotantovaatimukset ja niiden edellyttämä tietojen ylläpito
- poikkeusolojen vaikutus toimintaan
- organisaation omat olemassaolon vaatimukset kriisitilanteissa
- tietojenkäsittelyn keskeytysten vaikutus poikkeusoloissa
- päätoiminnan valmiustavoitteet
- tukitoimintojen valmiusvaatimukset
- ulkoistettujen toimintojen poikkeusolojen tarpeet
- tietotekniikan käytön supistaminen ja riippuvuuksien vähentäminen
- poikkeusoloissa tarvittava tietotekniikka ja tietotekniikkapalvelut
- turvallisuustoimenpiteet.

Tämä tarkistuslista on tarkoitettu tietoturvaluussuunnittelun, toipumissuunnittelun ja tietojenkäsittelyn poikkeusolojen suunnittelun apuvälineeksi.

PERUSTURVALLISUUS**TIETOTURVALLISUUSSUUNNITELMA****Analyysin yhteenveto**

- tietojenkäsittelyn merkitys elintärkeille toiminnoille
- häiriöiden seuraukset, vahinkojen suuruus ja vaikutukset erilaisissa tilanteissa
- turvallisuuden ja valmiuden taso
- johdon informointi analyysin tuloksista

Valmiuden tavoitteet ja kehittäminen

- hallinnollinen tietoturvaluus
- henkilöstöturvaluus
- tietoaineiston turvallisuus
- laitteistoturvaluus
- ohjelmistoturvaluus
- tietoliikenneturvaluus
- käytön turvallisuus
- fyysinen turvallisuus

Hallinnollinen tietoturvaluus – johtaminen

- elintärkeiden tietojärjestelmien ja sovellusten määrittely
- tietoturvaluusstrategia
- tietoturvaluuden yleisjärjestelyt ja toteutustapa
- vastuuorganisaatio, turvallisuusvastuut
- henkilöstön tehtäväkuvaukset
- tietoturvaluusperiaatteet ja -ohjeet

Henkilöstöturvaluus

- henkilöstöturvaluuden sisällyttäminen henkilöstöpolitiikkaan
- menettelyt palkattavan tietoteknisen henkilöstön luotettavuustarkistuksiin
- avainhenkilöiden sijaisuusjärjestelyt
- kirjalliset työsopimukset vaihtoluotettavuusvaatimuksineen
- menettelyt käyttöoikeuksien antamiseen ja välittömään poistamiseen erotilanteissa

Tietoaineistoturvaluus

- eheyden varmistaminen
- tiedon ja tietoaineiston käytettävyyden vaatimukset
- tietojen luokitus ja merkintä
- tietojen luokituksen mukaiset käsittely- ja säilytysäännöt, suojausmenettelyt
- tietoaineiston käyttövaltuudet
- salassapitosopimukset
- tietojätteen hävittäminen
- valvonnalle asetettavat vaatimukset

Laitteistoturvaluus

- laitteiden, varaosien ja tarvikkeiden hankintapolitiikka
- vikasietoisuus ja yhteensopivuus
- varalaitetarpeet
- saatavuuden varmistaminen sopimuksin

Ohjelmistoturvaluus

- eheys, luotamuksellisuus, käytettävyyden, todentaminen ja kiistämättömyys
- pääsynvalvonta ja käyttöoikeudet
- vähimmän valtuuden periaatteella määritellyt, tehtävien mukaiset pääsyovaltuudet

- salaus
- salasana- ja avainhallinnan määrittely, avainten suojaus
- tiedostojen suojaus
- tietokantojen ja prosessien eheyden hallinta tiedon luvattoman muuttamisen ja tuhoamisen estämiseksi
- järjestelmähallinnan turvallisuusvaatimukset
- varmuuskopioinnin, ohjelmajakelun, pääsyn- ja käytönvalvonnan, prosessien toiminnan ja käyttöympäristön valvonta
- työasemien, verkkojen ja tiedostojen suojaus, pääsynvalvonta, salaus ja virustorjunta
- ulkoistettujen palvelujen ja yhteyksien turvallisuusvaatimukset
- keskitettyjen resurssien – palvelimien, verkkoajan, nimi- ja hakemistopalvelujen - ja yhteyskäyttöketjujen tietojen sekä tiedonsiirtojärjestelmien toimivuuden varmistus

Tietoliikenneturvallisuus

- verkkoliittymien liityntä-, käyttö- ja turvallisuusperiaatteet
- ulkoisten verkkoliittymien turvallisuus, palomuuriratkaisut
- etähuoltoyhteyksien valvonta
- kytkentäisten verkkojen turvallisuuspalvelujen käyttö
- puhelinkytkentätilojen valvonta, teleoperaattorien henkilökunnan käytien valvonta
- verkkoihin pääsyn valvonta, luvattomien liityntäyritysten havainnointi ja raportointi
- tiedonsiirron suojaus
- verkon varayhteydet

Käyttöturvallisuus

- käytön valvonta
- ulkoistettujen käyttöpalvelujen turvallisuusvaatimukset ja menettelyjen valvonta
- tapahtumien havainnointi
- sovellusten omistajien hyväksymät varmuus- ja suojakopiointiratkaisut
- ohjelmistotuen, ylläpidon, kehittämisen ja huollon turvallisuustoimenpiteet
- vastuut ja menettelyt käyttöoikeuksien, käytön ja lokien valvontaan ja tapahtumien raportointiin
- koko tietojenkäsittelyn kattavan teknisen toimivuuden seuranta ja sen raportointi

Fyysinen turvallisuus

- fyysisen turvallisuuden tavoitteet
- laitteiden suojaustason määrittely
- käyttäjien, tietoteknisen henkilöstön, kiinteistönhoidon ja turvallisuushenkilöstön vastuut fyysisestä turvallisuudesta ja sen ylläpidosta
- rakenteellinen turvallisuus tietoteknisissä tiloissa ja säilytystiloissa
- valvontajärjestelmät ja niiden käyttö
- käytön varmistavat tekniset järjestelmät
- kone- ja palvelinhuoneiden olosuhdevalvonta ja hälytysten siirto
- valmiudet ongelmatilanteiden ja onnettomuuksien hallintaan pelastussuunnitelmien

Seuranta ja raportointi

- koko tietojenkäsittelyn avainkohtiin kohdistuva, yhtenäinen valvontamenettely
- olennaisten tapahtumien rekisteröinti ja raportointi
- menettelyt havaittujen puutteiden poistamiseksi

TOIPUMISSUUNNITELMA

Toipumisvalmiuden arvioinnin yhteenveto

Tilannearviot ja -kuvaus

- kuvaus vakaviin keskeytyksiin johtavista tapahtumista, erityistilanteet
- kriittiset tapahtuma-ajankohdat
- laitteiston, ohjelmistojen, tiedostojen, tietokantojen, tietoliikenteen ja oheislaitteiden käytettävyys ongelmatilanteissa
- tapahtumien vaikutukset tietojenkäsittelyyn, verkkopalveluihin, tietoliikenteeseen, vahinkojen laajuus
- tapahtumien vaikutukset päätoimintoihin
- keskeytysten vaikutukset tietojärjestelmien eheyteen ja käytettävyteen
- toimintojen ja palvelujen arviointi keskeytysten kannalta
- keskeytysten vaikutukset tuotantoon, palveluihin, asiakkaisiin ja toimituksiin
- toimintojen tietotekniikka- ja verkkoriippuvuudet
- palvelujen keskeytymisen vaikutukset muiden tahojen toimintaan
- kriittisiksi muodostuvat keskeytysajat
- kausiluonteiset kriittiset ajankohdat
- arviot keskeytystilanteessa syntyvistä taloudellisista menetyksistä
- keskeytyksistä aiheutuvien kokonaiskustannusten ja -vaikutusten arviointi
- tietotekniikan käytön rajoituksissa ylläpidettävien tietojärjestelmien ja sovellusten varmistamisen prioriteetit

Menetysten arviointi

- tuotannon menetykset
- tuottojen menetykset
- keskeytyksen aiheuttamat lisäkustannukset
- korkotappiot
- lisääntyneet vuokratulot
- välilliset kulut
- viivästymissakot
- asiakas- ja yrityskuvamenetykset ja
- keskeytysvakuutusten vaatimukset ja vaikutukset

Elintärkeät toiminnot ja palvelut

- elintärkeät, varmistettavat palvelut ja toiminnot
- elintärkeät tietojärjestelmät
- toimintojen suurimmat sallitut keskeytysajat
- toiminnan varmistamisen periaatteet

Johtopäätökset

- varajärjestelmätarve
- varajärjestelmään siirtymisen vaatimat ajat
- vahinkojen korjaamisesta ja normaaliin toimintaan palaamisen edellyttämät toimenpiteet palautumisaikoinen

Palvelutasovaatimukset

- päätoimintojen palvelutaso- ja tuotantovaatimukset ja niiden riippuvuus tietojenkäsittelystä ja tietoliikenteestä, ylläpitoon tarvittavat resurssit
- päätoiminnoille sallittu suurin hyväksyttävissä oleva keskeytysaika, tietojärjestelmien suurin sallittu toimintakato
- toimitusaikojen, tuottojen tai palvelun suurin hyväksyttävissä oleva heikkeneminen erilaisissa keskeytystilanteissa
- suurin sallittu tuotannon keskeytysaika
- suurin sallittu viive siirryttäessä korvaavaan varajärjestelmään
- pisin sallittu toipumisaika normaalitoimintaan palaamiseksi
- tietojärjestelmittäin määritellyt prioriteetit varajärjestelmän käyttöönotossa
- tiedostojen varmuus- ja suojakopioiden ajantasaisuus

Kriittisten tietojärjestelmien resurssitarpeen määrittely

- tarvittavat tietojärjestelmät ja tietokannat
- palvelimet, keskuslaitteet ja osajärjestelmien laitteet
- verkkopalvelut, verkot ja tietoliikenneyhteydet
- käyttötoiminnot
- tuki- ja huoltopalvelut
- hankinnat
- henkilöstö
- aika-arviot

Tietotekniikan varmistaminen

- elintärkeät tietojärjestelmät, sovellukset, verkot ja tietoliikenne
- kriittiset sovellukset, tietokannat ja tiedonsiirto
- hajautetut tiedot, tietokannat ja sovellukset
- tiedonkeruun ja tapahtumien tallennus
- valmius korvaavien järjestelmien käyttöön
- varajärjestelmätarpeet, laitteet, oheislaitteet ja tarvikkeet, muut resurssitarpeet
- käyttöjärjestelmä-, varusohjelmisto- ja sovellusohjelmistotarpeet
- ulkoistettujen palvelujen tarpeet, henkilöstötarpeet
- henkilökunnan käyttö
- tietoliikenteen varmistamis- ja ohjaustarpeet
- tietojenkäsittelyn varmistamisperiaatteet

Tiedostojen varmistaminen

- dokumentit laitteistosta ja ohjelmistoista
- käyttöjärjestelmien, tukiohjelmien, sovellusten, tiedostojen ja tietoliikenneohjelmistojen suojakopiointi/ replikointi
- ohjeet ja tiedostot järjestelmän ja sen osien uudelleen konfigurointiin

Varatila

- ratkaisuvaihtoehtojen vertailu
- varalaitteistoratkaisu
- sopimusperusteiset ratkaisut
- tilaratkaisut
- tilojen kunnostus

Tietoliikenteen varmistaminen

- varajärjestelmäkokonaisuuden tietoliikennetarpeet
- paikallisverkkojen varmistus
- etäverkkojen varmistus
- sopimukset tietoliikenteen vaatimista muutoksista ja liitännöistä
- tiedonkeruun vaatimat yhteydet
- muut vaihtoehtoiset tiedonsiirtotavat
- konfigurointi

Lähiverkot

- verkkopalvelimien varmistukset
- verkkopalvelimien varalaitteiden ja varaosien varaaminen
- valmiudet verkkojen ja verkon laitteiden korjaamiseen, korvaamiseen ja konfigurointiin
- valmius toiminnan siirtämiseksi muualta tapahtuvaksi

Toipumissuunnitelmaan siirtyminen

- kriittisen aineiston ja laitteiston pelastaminen
- toimenpideluettelo varajärjestelmän käytölle; päätöksenteko ja valmistelut
- varajärjestelmän pystytys-, käynnistys- ja käyttötoimenpiteet
- erityistilanteiden hallinta

Palaaminen normaaliin toimintaan

- periaatteet ja ratkaisut palautumiselle

- toimenpiteet tietotekniikan uudelleenrakentamiseksi
- tarvittavat valmistelut

Valmiusryhmä

- valmiusryhmän kokoonpano ja tehtävät
- yksiköiden vastuuhenkilöt
- vastuuhenkilöiden tehtävät toipumissuunnitelman toimeenpanossa
- sijaisuudet

Seuranta ja raportointi

- varajärjestelmiin vaikuttavien muutosten seuranta
- toipumisvalmiuden seuranta
- valmiuden raportointi
- uudet uhkatilanteet ja havaitut riskitekijät
- vahinkotapahtumien ja niiden vaikutusten käsittely
- raportointi teknisistä vioista ja häiriöistä
- parantavat turvallisuustoimenpiteet
- raportointi ylimmälle johdolle

Toipumissuunnitelman testaus

- testauskohteet ja laajuus
- testaustavat ja -tiheys
- raportointi tuloksista
- parantamistoimenpiteet

Tiedottaminen

- tiedotusperiaatteet
- tiedottamisen vastuut ja valtuudet
- ulkoisen ja sisäisen tiedottamisen pääpiirteinen sisältö
- tiedotuskanavat

Suunnitelman säilytys

- jakelu ja säilytys
 - säilytys suojakopioarkistossa
-

POIKKEUSOLOT

TIETOJENKÄSITTELYN POIKKEUSOLOJEN VALMIUSSUUNNITELMA

Poikkeusolojen valmius

- arvio yrityksen olemassa olevista edellytyksistä toimintaan eri asteisissa poikkeusoloissa
- arvio kriisinaikaisesta tietotekniikka- ja palveluriippuvuudesta
- henkilöresurssien arviot
- tietotekniikan käytettävyys poikkeusoloissa
- arviot tiedonsiirron keskeytyksistä
- arviot huollon, varaosien, tarvikkeiden ja palvelujen saannista ja riittävydestä poikkeusoloissa

Poikkeusolojen vaikutusten arviointi

- arvio eriasteisten poikkeusolojen vaikutuksista tietotekniikan käyttöön, henkilöstöön ja palveluihin
- arvio tietojärjestelmien ja tietoliikenteen riskialttiudesta, aroista sovelluksista ja tietokannoista
- kriittisten riippuvuuksien määrittely
- kuvaus poikkeusolojen vaikutuksista tuotantoon ja tietojenkäsittelyyn

Perusteet poikkeusolojen valmiudelle

- valmiussuunnittelun tavoitteet
- poikkeusoloissa ylläpidettävät toiminnot ja palvelut
- tietojärjestelmien tärkeysluokitus poikkeusolojen kannalta
- riippuvuudet alihankkijoista
- tarvikkeiden ja varaosien saanti/korvaaminen
- toimintojen supistamissuunnitelmat ja uudelleenjärjestelyt
- tietojärjestelmittäin määritelty ylläpidon taso ja valmiusvaatimus

Poikkeusolojen tietojenkäsittelyn toteutus

- toimintavaihtoehdot
- valmiussuunnittelun vastuut, organisaatio poikkeusoloissa
- varmistettavat järjestelmät ja resurssit
- laitteistokapasiteetin varaaminen
- varmuus- ja suojakopioiden säilytys ja käytön varmistaminen
- henkilöstön käyttö poikkeusoloissa
- henkilövarausten ylläpito ja henkilöstön koulutus
- varatila- ja varakeskusjärjestelyt

Laitteet, varaosat, tarvikkeet ja huolto

- varmistettavien järjestelmien määrittely
- varajärjestelmätarpeiden määrittely
- korjausmenettelyt
- varalaiteratkaisut
- korvaavat menettelyt
- varaosien ja tarvikkeiden varaaminen
- hankintamenettelyt
- selvitys kriittisistä laitetarpeista (tärkeysluokitellut organisaatiot)
- huoltojärjestelyt

Tietoliikenne

- tietoliikennevaatimukset
- tarvittavien tietoliikenneyhteyksien määrittely
- yhteysvaraukset käytettäviltä teleoperaattoreilta
- varajärjestelyt, vaihtoehtoiset tiedonsiirtotavat
- tietoliikennesuunnitelma

Vastuu

- poikkeusolojen tietojenkäsittelyn vastuut
- käyttöorganisaatio
- täydennykset toimenkuviin ja työjärjestyksiin

Henkilöstö

- henkilöstön poikkeusolojen käyttösuunnitelma
- periaatteet varausesitysten laatimiseksi
- varattavaksi esitettävien tärkeysjärjestys
- henkilöstön sijoittaminen vaihtoehtoisin tehtäviin
- sijaisuuksien järjestäminen ja niihin varautuminen
- koulutussuunnitelma

Ohjelmistot ja käyttö

- tukitarpeiden ja riippuvuuksien määrittely
- ratkaisut välttämättömän ohjelmiston ylläpidolle ja tuelle
- varmuus- ja suojakopioinnin uudelleenjärjestely
- ohjelmistojen, tietoliikenteen ja käytön turvallisuuden lisäykset

Fyysinen turvallisuus

- pelastussuunnitelmien tietojenkäsittelyä koskevat täydennykset
- keskeisten laitteistojen ja solmukohtien suojaustoimenpiteet
- muut suojausmenettelyt

Tietotekniikan käytöstä luopuminen

- keskittyminen kriittisiin järjestelmiin
- korvaavat menettelyt ja laitteet

Palaaminen normaalitoimintaan

- elpymisedellytysten ylläpito
- tekniset ja toiminnalliset edellytykset

Tiedottaminen ja yhteydet

- viranomaiset, alihankkijat

Valmiuden ylläpito ja tarkastaminen

- vuosittain
- muutosten yhteydessä
- vastuut

Valmiustilanteen seuranta ja raportointi

- menettelytapa
 - tason arviointi
 - kehittäminen
-