Tietoturvallisuus järjestelmäkehityksessä

Tärkeä perusta toimivalle tietoturvallisuudelle ovat laadukkaat, luotettavasti toimivat tietojärjestelmät, joihin on toteutettu riittävät, oikein mitoitetut turvatoimet. Tietoturvallisuusnäkökulma on syytä pitää esillä tietojärjestelmän elinkaaren kaikissa vaiheissa esitutkimuksesta järjestelmän käytöstä poistoon saakka. Tueksi toimivan tietoturvallisuuden rakentamiselle tietojärjestelmien kehittäjät tarvitsevat tietoa siitä, mitä turvatehtäviä järjestelmäkehityksen eri vaiheisiin tulisi sisällyttää. Aihetta on sen tärkeydestä huolimatta käsitelty kirjallisuudessa melko vähän. Tämän lehden sisältämien artikkelien tarkoituksena on antaa lukijoille perustiedot järjestelmäkehityksen turvatoimista. Lisäksi yhdessä artikkelissa käsitellään henkilön sähköisen tunnistamisen hanketta. Tämä on merkittävä tietoturvallisuuden infrastruktuurin kehittämishanke, jonka vaikutukset tuleva aikanaan ulottumaan laajalti kansalaisten elämään ja asiointiin mm. virastoissa.

Aiheen laajuudesta johtuen käsittelynäkökulmaa on jouduttu rajaamaan. Keskeisenä sisältönä on turvatoimien sijoittaminen järjestelmän elinkaaren eri vaiheisiin. Käsittelemättä jäävät muun muassa projektien hallintaan liittyvät riskit ja tietojärjestelmien laadun varmistaminen. Rajauksista huolimatta toivomme kokoamamme aineiston olevan järjestelmien kehittäjille käyttökelpoinen tietoturvallisuuden toteuttamisen apuväline ja antavan virikkeitä hankkia tarvittavia lisätietoja aiheesta.

Hellevi Huhanantti, Aarno Kansikas ja Helvi Salminen

Hellevi Huhanantti toimii Tietoleonia Oy:ssä järjestelmäpäällikkönä tietoturvatehtävissä. Hän on Tietoturva ry:n puheenjohtaja.
puh: 020425 5954
hellevi.huhanantti@leonia.fi

Aarno Kansikas toimii johdon konsulttina ICL Konsultoinnissa tärkeimpänä erityisosaamisalueenaan tietoturvallisuuden kehittämisprosessi. Hän on myös Tietoturva ry:n hallituksen jäsen.
puh. 09-567 3450
aarno.kansikas@icl.fi

Helvi Salminen toimii tietoturva-asiantuntijana Setec Oy:ssä. Tärkeimpänä vastuualueena on yrityksen sisäisen tietoturvallisuuden kehittäminen. Tietoturva ry:n hallituksessa Helvin tehtävinä ovat yhdistyksen taloudenhoito ja koulutustoiminta.
puh. 09-8941 4341
helvi.salminen@setec.fi

SYSTEEMITYÖ 3/98

Pääkirjoitus:

Mikä on Tietoturva Ry - Finnish Information Security Association

Hellevi Huhanantti,
Järjestelmäpäällikkö,
Tietoleonia Oy

Yhdistyksen perustaminen

TIETOTURVA RY, eräs Tietotekniikan liiton valtakunnallisista teemayhdistyksistä perustettiin syksyllä 1997. Yhtenä yhdistyksen perustamisen syynä oli muodostaa valtakunnallinen tietoturva-alan ammattilaisten foorumi.

Tietoturvallisuus on yrityksissä nousemassa verkottumisen myötä yhä merkittävämpään asemaan. Tietoturvallisuuden kasvu on myös nähtävissä tietoturvallisuustuotteiden lisääntyvänä tarjontana sekä ammattilaisten kysyntänä. Computer Security Institute on arvioinut, että Yhdysvalloissa tietoturva-asiantuntijoiden määrän kasvu on n. 17 % tänä vuonna. Yhdistyksen perustamiselle olikin olemassa otollinen maaperä.

Toiminta vuonna 1998

Yhdistyksen varsinainen toiminta alkoi vuoden 1998 alusta ja henkilöjäsenten määrä oli elokuussa 1998 noin 150 ja yhteisöjäsenten määrä kaksi. Olemme saavuttaneet hallituksen ensimmäiselle vuodelle asettamat jäsenmäärätavoitteet. Yhdistyksen valtakunnallinen toiminta ei ole vielä käynnistynyt, mutta olemme organisoimassa sitä vielä tämän vuoden aikana. Tavoitteenamme on pitää ainakin yksi koulutustilaisuus pääkaupunkiseudun ulkopuolella yhteistyössä Tietotekniikan liiton paikallisyhdistysten kanssa.

Tietoturva ry:n vuoden 1998 toimintasuunnitelman tavoitteita ovat:

- edistää ja kehittää tietoturvallisuutta ja hyvien tietoturvallisuustapojen noudattamista tietoturvallisuuden kaikilla osa-alueilla
- toimia jäsentensä yhdyssiteenä ja edistää yhteistoimintaa
- tukea jäsentensä pyrkimyksiä kehittää ja ylläpitää tietoturvallisuustoiminnan ammattitaitoa ja laatua.

Tavoitteidensa toteuttamiseksi yhdistys

- järjestää tietoturvallisuuden koulutus-, julkaisu- ja tutkimustoimintaa
- seuraa tietoturvallisuuden kotimaista ja kansainvälistä kehitystä
- pitää yhteyttä muihin järjestöihin, tietoturvallisuuskoulutusta antaviin oppilaitoksiin ja muihin tietoturvallisuuden vaikuttajatahoihin Suomessa ja ulkomailla toimien näiden kanssa yhteistyössä tietoturvallisuuden edistämiseksi.

Tietoturva ry:n hallituksen kokoonpano	
Tietoturva ry:n hallitus valitaan vuodeksi kerrallaan syyskokouksessa. Yhdistyksen hallitus koostuu puheenjohtajasta, varapuheenjohtajasta, varainhoitajasta ja kahdesta neljään muusta jäsenestä. Ensimmäisen toimintavuoden hallitukseen valittiin seuraavat seitsemän jäsentä:	**Puheenjohtaja** Hellevi Huhanantti Tietoleonia Oy Kaupintie 3, 00007 Helsinki puh. 09-8595 0747, 040-501 0250 fax 09-8595 0753 email:hellevi.huhanantti@leonia.fi
Varapuheenjohtaja+tiedotus Petri Väänänen QA Information Security Oy Sinikalliontie 9, 02630 Espoo puh. 09-527 07210 fax 09-527 07100 email:petri.vaananen@qainfo.fi	**Web-vastaava** Aarno Kansikas ICL Data Oy Pl 458, 00101 Helsinki puh. 09-567 3450, 050-597 1320 email:aarno.kansikas@ icl.fi
Varainhoitaja, koulutusvastaava Helvi Salminen Setec Oy Pl 31, 01741 Vantaa puh. 09-8941 4341, fax 09-891 887 email:helvi.salminen@setec.fi	Tiina Danilotschkin-Forsman Sampokonserni Riskienhallintatoiminto, 000035 Teollisuusvakuutus puh. 010514 5710, 0500-327 052 fax 010514 5841 email:tiina.danilotschkin-forsman@tiimi.teva.elisa.fi
Pekka Ekman TT-Professional Solution Oy Piispantilankuja 4, 02240 Espoo puh. 09-3294 7622 fax 09-332349 7695 email:pekka.ekman@ttpro.fi	Anne-Maria Yrjänä Tietoleonia Oy Kaupintie 3, 00007 Helsinki puh. 09-8595 0432 fax 09-8595 0753 email:anne-maria.yrjana@ leonia.fi

Yhdistyksen järjestämät tapahtumat

Tietoturva ry on tänä vuonna järjestänyt kaikille avoimia koulutus- ja teematilaisuuksia sekä vain jäsenille tarkoitettuja jäsentilaisuuksia. **Tulevan syksyn tapahtumakalenterimme on seuraava:**

14.-15-10.98	**Secum-turvamessut, jossa järjestämme "Toimikortti tietoturvakäytössä" seminaarin samansisältöisenä molempina päivinä. Toimitamme jäsenillemme messujen kutsukortin, jolla pääsee messujen lisäksi myös seminaariin. Seminaarohjelma on jäljempänä tässä lehdessä.**
18.11.98	**CISSP-koulutusta ja –tutkintoa esittelevä seminaari. Luennoijana Virgil Gibson USA:sta**
19.11.98	**Ulkoistettujen tietotekniikkapalvelujen turvallisuutta sekä tietoturvallisuuden tason mittaamista käsittelevä seminaari, joka järjestetään yhteistyössä Tietojärjestelmien tarkastus ja valvonta ry:n kanssa.**
7.12.1998	**Yhdistyksen sääntömääräinen syyskokous**

CISSP-koulutus ja tutkinto

Tietoturva ry järjesti yhdessä Tietotekniikan liiton kanssa International Information Systems Security Certification Consortiumin $(ISC)^2$ kehittämän kansainvälisen tietoturvatutkinnon.Tämä on ollut yhdistyksen laajin koulutushanke.

Tutkintotilaisuuksia on järjestetty Yhdysvalloissa jo useita vuosia ja nyt tutkinto on kehitetty täyttämään kansainvälisen tutkinnon vaatimukset. Otimme vastaan $(ISC)^2$ -organisaation tarjoaman mahdollisuuden järjestää tutkintotilaisuus ensimmäisenä Euroopassa.

Tutkinnon osa-alueet:

- **pääsynvalvonta**
- **tietoliikenteen turvallisuus**
- **riskienhallinta ja liiketoiminnan jatkuvuussuunnittelu**
- **tietoturvapolitiikat, standardit ja organisaatiot**
- **tietokonearkkitehtuurit ja systeemien turvallisuus**
- **etiikka, lait ja tutkinta**
- **sovellusohjelmien turvallisuus**
- **kryptografia**
- **käyttötoiminnan turvallisuus**
- **fyysinen turvallisuus.**

Tutkinto on tarkoitettu

- tietoturva-asiantuntijoille, joilla on vähintään kolmen vuoden työkokemus joltain yllälueteltuista alueista
- tietoturva-asiantuntijoille, joilla on usean vuoden työkokemus ja jotka aikovat kansainvälisille työmarkkinoille.

Syksyn 1997 kurssi ja kevään 1998 tutkinto

Tutkintoa varten järjestimme viiden päivän mittaisen valmennuskurssin marraskuussa 1997. Luennoitsija oli USA:sta ja kurssilla käsiteltiin kaikki yllä luetellut osa-alueet. Tämän lisäksi järjestimme myös kurssialueelta useita teematilaisuuksia. Muutama kuukausi valmennuskurssin jälkeen järjestimme kuuden tunnin mittaisen 250 monivalintakysymystä sisältävän tutkintokoetilaisuuden toukokuussa 1998. Kurssin luennot ja tutkintoon liittyvä koe olivat englanninkielisiä.

Tällä hetkellä on tutkinnon suorittaneita yhteensä noin 1200, joista suomalaisia on 19. CISSP-tutkinnon kansainvälistämisprojekti jatkuu ja seuraava Yhdysvaltain ulkopuolella järjestettävä tutkinto pidetään syyskuussa Irlannissa. **CISSP-kokeen läpäisi Suomessa yli 80 % kokelaista**.

Tulos oli hyvä verrattuna amerikkalaisten läpäisyprosenttiin, joka on noin 70. Kevään aikana USA:ssa tutkintokokeeseen osallistui 322 ja Suomessa 22 tietoturva-ammattilaista.

CISSP-hankkeen jatkosta

Tietotekniikan liitto neuvottelee seuraavasta CISSP-tutkintokurssin toteuttamisesta. Tavoitteenamme on pitää seuraava valmennuskurssi maaliskuussa 1999 ja tutkintokoe toukotai kesäkuussa 1999.

Lisätietoja

Lisätietoja yhdistyksestä, sen koulutustoiminnasta ja tilaisuuksista saat yhdistyksen kotisivuilta osoitteesta: ***www.ttlry.fi/tietoturvary***.

CISSP-tutkinnosta saat lisätietoja yhdistyksen hallitukselta ja ISC2:n kotisivuilta osoitteesta ***www.isc2.org/isc2.htm***.

Yhdistyksen hallitukselle voit lähettää sähköpostia osoitteeseen **tietoturva@ry.inet.fi**

Tietoturvallisuus järjestelmäkehityksessä - miksi ?

Helvi Salminen,
Tietoturva-asiantuntija,
Setec Oy

Tietoturvallisuus ei ole yksinomaan turvallisuuteen erikoistuneiden asiantuntijoiden päänsärky. Tärkeä rooli turvallisten tietojärjestelmien rakentamisessa on niiden kehittäjillä. Turvallisuuden toteuttaminen järjestelmiin jälkikäteen "päälle liimaamalla" on hankalaa, jopa mahdotonta. Siksi tietoturvanäkökulman on syytä olla mukana järjestelmän elinkaaren kaikissa vaiheissa alkaen esitutkimuksesta päätyen järjestelmän käytöstä poistamiseen.

Tietotekniikkariippuvuuden vaikutuksesta toiminnan haavoittuvuuteen

Nykypäivänä on vaikea kuvitella yritystä tai julkishallinnon organisaatiota, jonka toiminta ei olisi riippuvaista tietotekniikasta. Esimerkiksi nykyaikainen pankkitoiminta ei olisi mahdollista ilman kehittynyttä tietotekniikkaa. Teollisuusyritykset alihankkijoineen muodostavat monimutkaisia toimintoketjuja, jotka pidetään tietotekniikan avulla hallinnassa niin että oikeat asiat tapahtuvat oikeassa paikassa "just on time". Julkishallinto hyödyntää tietotekniikkaa omissa toiminnoissaan …

Tietotekniikka onkin monipuolinen ja hyödyllinen apuväline, jos tietojärjestelmät täyttävät niille asetetut tehtävät, toimivat luotettavasti ilman häiritseviä käyttökatkoja (*saatavuus*), niiden sisältämä tieto on oikeaa ja ajantasaista (*eheys*) eikä joudu asiattomien haltuun (*luottamuksellisuus*).

Tietojärjestelmien haavoittuvuutta lisäävä vaikutus perustuu siihen, että ne ovat merkittäviä organisaation tieto-omaisuuden keskittymiä. Monet toimintaprosessit on suunniteltu tietotekniikan varaan ja vastaavien toimintojen toteuttaminen manuaalisesti voi olla mahdotonta tai liian kallista. Siksi tietotekniikkaan tukeutuvan yrityksen on tärkeää luoda toimivat varajärjestelmät.

Tietotekniikan käyttöön liittyvään toiminnan haavoittuvuuteen on syytä suhtautua vakavasti. Tärkeän tietojärjestelmän tuhoutuminen voi pahimmillaan vaarantaa organisaation olemassaolon. Jos järjestelmän tietosisältö rapautuu, organisaatiossa voidaan tehdä virheellisen tiedon perusteella vääriä päätöksiä ja kaaos on valmis. Jos asiaton taho pääsee käsiksi tietojärjestelmän sisältämiin liikesalaisuuksiin, organisaatio voi menettää kilpailukykynsä.

Keskeisiä tietoturvauhkia

Tietoturvallisuuteen kohdistuvat uhkat voivat olla peräisin organisaation sisältä tai ulkoa. Sisäisiä uhkia ovat esimerkiksi:

- Tietojärjestelmän huono laatu ja puutteelliset kontrollit
- Järjestelmien riittämätön dokumentointi
- Puutteelliset järjestelmien käyttöohjeet
- Huonosti hoidetut varmistukset
- Varmistusten testaamattomuus
- Jatkuvuussuunnittelun puutteet
- Välinpitämättömyys ja huolimattomuus tietojen käsittelyssä
- Tietoturvauhkia ei tunnisteta eikä niihin ole millään tavoin varauduttu
- Organisaation epäselvä vastuujako ja vakiintumattomat toimintatavat
- Liian vähäiset henkilöresurssit ja kiireen myötä lisääntyvät turvatoimien laiminlyönnit ja virheet
- Henkilöstön tahalliset tietoturvaa vaarantavat toimenpiteet

Ulkoisia uhkia ovat mm:

- Yritysvakoilu
- Rikollisuus
- Laite- ja ohjelmistohuollon toimimattomuus
- Luonnontapahtumista (ukkonen, tulvat, ...) toiminnalle aiheutuvat vahingot
- Muut yrityksen toimintaympäristöön liittyvät ongelmat

Kenellä vastuu tietoturvallisuudesta

Tietoturvallisuus ei valitettavasti hoidu itsestään. Se ei myöskään ole pelkästään tekninen ongelma, joka on ratkaistavissa teknisin keinoin. TT:n PKT-valtuuskunnan puheenjohtaja Jalo Paananen totesi keväällä 1998 pitämässään esityksessä, että tietoturvallisuus on johtamisongelma, jota valitettavan usein yritetään ratkaista ainoastaan teknisin toimenpitein.

Hyvin hoidetun tietoturvallisuuden yksi tärkeimmistä edellytyksistä on se, että organisaatio määrittelee tietoturvallisuuteen liittyvät vastuut. Seuraavassa muutamia ajatuksia siitä, mitä nämä vastuut voisivat olla järjestelmäkehityksessä.

Organisaation johdon vastuu

Organisaation johdon asia on määritellä, millainen tietoturvataso on riittävä ja tarkoituksenmukainen. Johdon tehtäviin kuuluu myös määritellä, kuva vastaa käytännön tietoturvasta sekä taata riittävät resurssit tietoturvallisuuden toteuttamiseen.

Tietoturva-asiantuntijoiden vastuu

Tietoturvallisuuteen erikoistuneiden henkilöiden tehtävänä on mm.

- hankkia organisaatiolleen ajankohtaista tietoa siitä, mitkä ovat tietoturvan toteuttamisen keinoja
- auttaa järjestelmien kehittäjiä tietoturvallisuutta koskevissa asioissa
- laatia tietoturvallisuuden "normeja" ja ohjeistusta johdon määrittelemän toimintapolitiikan mukaisesti
- huolehtia tietoturvakoulutuksesta organisaatiossa

Järjestelmän tilaajan vastuu

Järjestelmän tilaaja määrittelee toteutettavan järjestelmän tietoturvatason. Tilaajan vastuulla on myös valvoa, että sovittu taso on saavutettu.

Järjestelmän tekijän vastuu

Järjestelmän tekijöiden tärkeimpiä tietoturvatehtäviä ovat mm. seuraavat:

- Tekijä tutustuu huolella toiminnan vaatimuksiin, jotka sitten kuvataan järjestelmän toiminnallisiksi määrityksiksi
- Kehitystyön aikana pitää mielessä, miten parhaiten toteuttaa tietoturvallisuuden keskeiset elementit: saatavuuden, eheyden ja luottamuksellisuuden.
- Noudattaa organisaatiossa sovittuja työmenetelmiä
- Tekee huolellista ja laadukasta työtä ja testaa työnsä tulokset
- Dokumentoi työnsä tulokset
- Laatii hyvät käyttöohjeet

Huonosti hoidetun tietoturvallisuuden seurauksista

Tietoturvallisuuden pettämisestä aiheutuu yleensä aina jonkin verran kustannuksia. Vahingon välittömien kustannusten lisäksi voi seurauksena olla yrityskuvan heikkeneminen ja asiakkaiden menettäminen. Tietojärjestelmien puutteellisesta turvallisuudesta aiheutuvilta vahingoilta vältytään parhaiten ottamalla tietoturvallisuus huomioon jo esitutkimusvaiheessa.

Jos tietoturvallisuutta ei oteta huomioon järjestelmän kehittämisen alkuvaiheessa, se saatetaan joutua toteuttamaan jälkikäteen. Tästä aiheutuu ylimääräistä työtä ja mahdollisesti suuriakin lisäkustannuksia. Jälkikäteen toteuttaminen ei välttämättä ole helppoa. Ongelmia saattaa tulla esimerkiksi kehitystyökalujen aiheuttamista rajoitteista tai laiteympäristöstä, johon ei ehkä ole saatavissa vaatimusten mukaista turvatekniikkaa.

Järjestelmiin toteutettavat vahinkoja ehkäisevät, paljastavat ja korjaavat kontrollit on suunniteltava huolella ja vaatimusten mukaisesti. Puutteelliset kontrollit voivat johtaa siihen, että järjestelmä käytön aikana oireilee erilaisina ongelmina, esimerkiksi tiedon eheyden vähittäisenä pettämisenä. Vahinkoa on joskus erittäin vaikea korjata. Ongelmien ikävä puoli on, että ne usein ilmenevät tietojen vähittäisenä korruptoitumisena. Virheellistä tietoa ehditään pahimmassa tapauksessa tallentaa useisiin varmistussukupolviin ennen ongelman havaitsemista. Näin ollen on vaikea arvioida, mikä varmistussukupolvi kannattaa palauttaa tuotantoon.

Vuosi 2000 - vieläkö jotain on tehtävissä

Tietojärjestelmien tuomionpäivä lähestyy - tämän lehden ilmestyessä aikaa vuosituhannen vaihtumiseen on noin 450 päivää. Ongelmiin törmätään monissa järjestelmissä jo reilusti ennen H-hetkeä.

Tämän Y2K-ongelman vakavuus ja mittasuhteet on, kiitos harjoitetun tiedotustoiminnan, alettu ymmärtää varsin laajasti. Organisaatiolla, joka vasta nyt herää ruususen unestaan, on suuria vaikeuksia saada järjestelmissä piilevät ongelmat kartoitetuksi ja löytää resursseja tarvittavien korjausten tekemiseen. Niissäkin organisaatioissa, joissa Y2K-projekti on ollut käynnissä jo hyvän aikaa, osa ongelmista jäänee hoitamatta.

Jos kaikkia vuosituhannen vaihteen tuomia ongelmia ei ehditä hoitaa, ongelmat pitää asettaa tärkeysjärjestykseen. Vähemmän tärkeät järjestelmät voidaan päättää jättää suosiolla entiselleen, mutta päätöksen on perustuttava järjestelmän merkitykseen, ei satunnaisiin asioihin. Järjestelmien väliset liittymät voivat aiheuttaa ikäviä yllätyksiä. Saattaa käydä niin, että Y2K-valmiuteen saatettu sovellus käyttää lähtötietoinaan aineistoa, jonka tuottavan sovelluksen Y2K-valmiuksia ei ole pidetty tärkeänä.

Paras asiantuntemus tai kyky ottaa selvää näistä järjestelmien keskinäisistä riippuvuuksista on järjestelmien kehittäjillä. Heidän tehtävänsä on informoida ongelmista organisaation liiketoiminnasta ja riskienhallinnasta vastaavia päätöksentekijöitä.

Mistä lisää tietoa järjestelmäkehityksen turvallisuudesta

Kattavaa esitystä siitä, miten rakentaa turvallisia järjestelmiä, eivät tämän lehden toimitustyöhän osallistuneet henkilöt ole löytäneet. Olemme koonneet mielestämme tärkeimpiä asioita, joiden avulla systeemityön ammattilainen saa kohtalaisen yleiskuvan ongelmakentästä ja joitakin viitteitä tietoturvallisuuden huomioonottamisesta järjestelmäkehityksessä.

Tietoturvallisuuden perusteoksista löytyy lyhyehköjä jaksoja tämän teeman tiimoilta. Oman organisaation käyttämässä systeemityömallissa otetaan mahdollisesti kantaa myös turvallisuuskysymyksiin. Jos organisaatiolla on käytettävissään tietoturvallisuuden ammattilaisia, nämä tuovat kehitystyöhän näkemyksensä siitä, mitä organisaation turvallisuuspolitiikka vähintäänkin vaatii tehtäväksi.

Kehitystyötä tekevän ammattitaito on toimivan, turvallisen järjestelmän välttämätön edellytys. Hyvät suunnitelmat, huolellinen toteutus ja kattava testaus varmistavat parhaan mahdollisen lopputuloksen.

Lisätietoja aiheesta

Hetky tietoturvakerho, *Sovelluskehitys ja tietoturvallisuus*, 1994

Tulosturva Oy, *RISTO-ohjelmisto versio 10.1*, 1998

Instrumentointi Oy, *SecGO Tutor – ohjelmisto versio 3.0*, 1998

Mikael Salonaho, *Suomen tietoturvallisuutta käsittelevän kyselytutkimuksen tulokset*, 1994

Tietoturvallisuutta käsittelevä kirjallisuus yleisesti

Tietoturvallisuuden keskeisiä käsitteitä

Helvi Salminen,
Tietoturva-asiantuntija,
Setec Oy

Tietoturvallisuuden terminologia ei ole täysin vakiintunutta. Seuraavassa on muutamia keskeisiä tietoturvallisuuden käsitteitä, joita esiintyy tämän lehden artikkeleissa.

Käsitteiden määrittely

Tietoturvallisuus (tietoturva) on tietojen, järjestelmien ja palveluiden asianmukaista suojaamista sekä normaali- että poikkeusoloissa lainsäädännön ja muiden toimenpiteiden avulla. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai tahallisten, tuottamuksellisten ja tapaturmaisten inhimillisten tekojen aiheuttamilta uhkilta ja vahingoilta.

Saatavuus (käytettävyys) Järjestelmien tiedot ovat tarvittaessa niihin oikeutettujen käytettävissä.

Eheys Tiedot ja järjestelmät ovat luotettavia, oikeellisia ja ajantasaisia, eivätkä ne ole laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet virheellisiksi.

Luottamuksellisuus Tiedot ovat vain niiden käyttöön oikeutettujen saatavissa eikä niitä paljasteta tai muuten saateta sivullisten käyttöön.

Uhka Olosuhde, tapahtuma tai jokin taho, joka voi aiheuttaa vahinkoa organisaation resursseille. Uhka voi sisältyä johonkin resurssiin (on resusrssin ominaisuus) tai kohdistua resurssiin.

Riski on yhdistelmä vahingollisen tapahtuman todennäköisyyestä ja tapahtuman seurauksista.

Tietojen turvaluokitus on tietojen jakamista ryhmiin. Luokitteluperusteena käytetään yleisimmin tiedon luottamuksellisuutta. Tietoja voidaan luokitella myös eheyden tai saatavuuden mukaan. Sovitun luokan perusteella määritellään vaatimukset tiedon käsittelymenettelyille.

Tämän lehden artikkelissa *Tietoturvallisuusluokitukset* kerrotaan lisää tietojen, järjestelmien, toimitilojen ja käyttäjien luokituksista sekä luokitteluprosessista.

Tunnistaminen Menettely, jolla yksilöidään tietojärjestelmän jokin komponentti, käyttäjä tai laite.

Todentaminen Käyttäjän, laitteen tai muun tietojärjestelmän olion identiteetin varmistaminen.

Kiistämättömyys Kiistämättömyydellä tarkoitetaan sitä, ettei tekijä voi jälkikäteen kiistää tekemäänsä toimenpidettä.

Esimerkiksi viestin vastaanottaja ei voi kiistää lähettäneensä viestiä tai vastaanottaja viestin vastaanottamista.

Riskienhallinta on suunnitelmallista ja jatkuvaa toimintaa, jonka tavoitteena on tunnistaa ja analysoida riskit sekä hallita niitä tarkoituksenmukaisella tavalla. Riski hallitaan poistamalla, pienentämällä, hyväksymällä tai siirtämällä se.

Jatkuvuussuunnitelma sisältää ohjeet toiminnan jatkuvuuden turvallisesta mahdollisten häiriöiden aikana ja niiden jälkeen.

Toipumissuunnitelma on jatkuvuussuunnitelman osa, joka sisältää ohjeet varajärjestelyihin siirtymisestä ja toiminnan jatkamisesta varajärjestelmien avulla sekä palaamisesta normaaliin toimintaan.

Lisää määritelmiä

Hetky tietoturvakerho / Salminen Helvi (toim.), *Tietoturvallisuus etätyössä*, Suomen Atk-kustannus 1997

Hetky tietoturvakerho, *Tietoturvasanasto*, 1992

Tulosturva Oy, RISTO-ohjelmisto versio 10.1, 1998

Valtionhallinnon tietoturvallisuuden johtoryhmä, *Valtionhallinnon tietoturvallisuuskäsitteistö*, http://www.vn.fi/vm/suomi/muuta/vahti/sanasto.htm

Instrumentointi Oy, SecGO Tutor –ohjelmisto V3.0, 1998

Toimikortti tietoturvallisuuskäytössä – seminaari SECUM 1998-tapahtumassa

Tietoturva ry järjestää SECUM-näyttelyn yhteydessä toimikortteihin keskittyvän tietoturvaseminaarin. Seminaari järjestetään samansisältöisenä molempina messupäivinä 14. ja 15.10.1998. Messujen asiakaskortilla pääsee myös kuuntelemaan tässä seminaarissa esiintyvien asiantuntijoiden puheenvuorot.

Toimikorttiteknologian perusasioita

10:00-10:10	***Seminaarin avaus,*** Tietoturva ry / Tietotekniikan liitto
10:10 - 11:00	***Toimikorttien keskeiset käyttöalueet ja kehitysnäkymät*** Petteri Hämäläinen, Setec Oy
11:00 - 12:00	***Toimikorttien turvallisuus*** Lauri Paatero, Setec Oy

Toimikortti tietoturvallisuuskäytössä

13:00-13:40	***Julkisen avaimen infrastruktuuri ja toimikortit*** Hannu Koukkula, IS-Comsec Oy
13:40-14:20	***HST-(Henkilön sähköinen tunnistaminen) -hanke Suomessa*** Ari Saapunki, Väestörekisterikeskus
14:20-15:00	***Toimikortin käyttömahdollisuuksia tietoturvaratkaisuissa*** Aarno Kansikas, ICL

Tulevaisuuden tekniikkaa ja uusia ratkaisuja

15:10-15:40	***Java cards today and in future*** Isabelle Pradier, Bull
15:40-16:20	***How to meet different security requirements with one single smart card solution today,*** Jan T. Johansen, ActivCard
16:20-16:30	***Loppuyhteenveto*** Tietoturva ry / Tietotekniikan liitto

Tietoturvallisuusluokitukset

Aarno Kansikas,
Johdon konsultti,
ICL Konsultointi

Rekisteröidyn tiedon määrä kasvaa jatkuvasti. Samalla järjestelmien käyttöhäiriöistä aiheutuvat ongelmat lisääntyvät, väärinkäyttömahdollisuudet lisääntyvät ja tietoturvallisuusuhat kasvavat, jolloin riskien torjunta tulee entistä tärkeämmäksi ja entistä enemmän resursseja vaativaksi.

Jotta turvallisuuden ja erityisesti tietoturvallisuuden (tietämysturvallisuuden) kehittämiseen tähtäävät toimenpiteet voidaan kohdistaa optimaalisesti on mm. tiedot, tietojärjestelmät, tilat, omaisuus, viestivälineet ja käyttäjät luokiteltava, ja mieluiten jo järjestelmien kehitysvaiheessa. Tätä työtä ei yleisesti ole tehty ja siksi siitä seuraakin oma ylimääräinen kehitysprosessinsa. Usein rajalliset tietoturvallisuustoimenpiteet ja resurssit voidaan luokitusten avulla kohdentaa tärkeimpiin kohteisiin eli panostaa oikein. Tällöin niiden vaikutukset ovat myös tehokkaimmat.

Luokittelu on yksi loogisen tietoturvallisuuden tärkeimmistä menetelmistä.

Tärkeysluokitukset

Toimintojen (ydinprosessien) tärkeysluokittelu sisältää tietojärjestelmien ja niissä käsiteltävien tietojen, usein myös organisaatioiden ja niiden toimitilojen sekä henkilöstön luokittelun.

Tietojen luokituksen tarkoituksena on jakaa tiedot ryhmiin, joille voidaan asettaa käsittelysäännöt. Oleellista on määritellä tietojen kriittisyys (arvo, tärkeys) ja toisaalta luottamuksellisuus, eheys ja käytettävyys.

Optimaalinen tietoturvallisuuden kehittäminen monen, toiminnaltaan melko itsenäisen toiminnon muodostamassa hajautettujen toimintojen ja tietojenkäsittelyn ympäristössä edellyttää konkreettisten normien eli luokitusten määrittämistä.

Tietojen luokittelu

Luottamuksellisuusluokitus

Tietoaineiston yhtenäinen käsittely edellyttää, että sen arvioinnilla ja luokittelulla on yhtenäiset lähtökohdat. Lähtökohtia asettavat ennen kaikkea aineiston merkitys organisaatiolle ja sen suojaustarve sekä sovellettavat säädökset, määräykset, sopimukset ja vastaavat.

Kunkin organisaation on määriteltävä tapauskohtaisesti, mitä säädöksiä, määräyksiä ja vastaavia tulee soveltaa aineistoja luokiteltaessa. Yksityissektori voi hyödyntää soveltaen oheisia julkishallinnon suositusluonnoksia.

Kaikkia valtionhallinnon organisaatioita koskevat ainakin julkisuutta, tietosuojaa ja salassapitoa koskevat säädökset ja määräykset. Lisäksi useimpia organisaatioita koskee valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä.

Julkisuuslainsäädännön ja salassapitosäädösten pohjalta arvioidaan, onko tietoaineisto julkista vai salassa pidettävää;

* Julkiseksi aineisto luokitellaan, mikäli sitä ei julkisuuslain tai muun säädöksen perusteella ole määritelty salassapidettäväksi.

* Salassa pidettäväksi aineisto luokitellaan, mikäli se on julkisuuslain tai muun säädöksen perusteella määritelty sellaiseksi.

Salassa pidettävä aineisto arvioidaan ja luokitellaan tietoturvallisuus- ja tietosuojanäkökohtien perusteella. Aineisto luokitellaan sen mukaan, minkälaisia seurauksia salassa pidettävän tiedon paljastuminen ulkopuolisille ja sen väärinkäyttö aiheuttaa suojattaville intresseille.

* Luottamukselliseksi aineisto luokitellaan, mikäli tiedon paljastumisesta ulkopuolisille (yksityisille ja julkishallinnolle) aiheutuu haitallisia seurauksia.

* Salaiseksi aineisto luokitellaan, jos tiedon paljastumisesta aiheutuu (yksityisille ja julkishallinnolle) huomattavia haitallisia seurauksia.

* Erittäin salaiseksi aineisto luokitellaan, mikäli tiedon paljastumisella on (yksityisille ja julkishallinnolle) erittäin haitallisia seurauksia.

Tätä perusluokitusta voivat täydentää salassapidettävien tietojen osalta toiminto- ja organisaatiokohtaiset erityisluokitukset esimerkiksi “Sisäinen“-luokka “Luottamuksellisen“ kahtiajakoon tai omana luokkanaan.

Kukin toiminto/organisaatio voi tarkentaa, määrittää ja "asettaa" omat erityisluokkansa edellä mainittujen luokkien mukaisesti.

Kukin organisaatio arvioi ja luokittelee saamansa tai itse laatimansa aiemmin luokittelemattoman tietoaineiston. Aiemmin muualla luokitellun aineiston luottamuksellisuusastetta ei saa lieventää.

Eheysluokitus

Tietojen luokitus eheyden perusteella voidaan luoda ydinprosessien määrityksessä esim. jäljempänä olevasta taulukosta ilmenevällä tavalla tai määrittämällä luokitus tarvittaessa osa-alueittain “ristiin“.

Tietojen luokitus eheyden perusteella tullee jatkossa olemaan osa EU:ssa kehitettävää sovellusten sekä palvelujen luokitusta ja standardointia. Perusteina käytettävää normistoa ollaan luomassa osaksi kansainvälistä *Common Criteria* -normistoa.

Eheysluokitukset on määriteltävä tarkoitukseen soveltuvalla tavalla organisaatiokohtaisesti (esimerkki: ajantasaisuus, laatu, varmistukset)

1. Luokka: tosiaikainen, tarkastetut tiedot, 1 kertaa /vrk
2. Luokka: vuorokausi, tarkastetut tiedot, 2 kertaa /viikko
3. Luokka: viikko, ei tarkastetut tiedot, 2 kertaa /kk

Käytettävyysluokitus

Tietojen ja tietoteknisten sovellusten luokitus käytettävyyden perusteella voi olla esim. seuraavanlainen. Kunkin organisaation on luotava oma tarkoitukseensa soveltuva luokitus: (Esim. kriittisyys ja toiminnon sallittu käytöstä poissa olo)

1. Erittäin kriittiset tiedot ja järjestelmät: minuutteja
2. Kriittiset tiedot ja järjestelmät: tunteja
3. Vähän kriittiset tiedot ja järjestelmät: 1- 2 päivää
4. Ei-kriittiset tiedot ja järjestelmät: enintään 1 viikko
5. Vähemmän tärkeät tiedot ja järjestelmät: viikkoja - kuukausia

Kriittisyys voi vaihdella ajankohdan ja käyttötarpeen mukaan. Toiminnon poissaoloa voidaan tarpeen mukaan arvioida muun muassa huippuarvojen, keskiarvojen, mediaanien avulla. Usein saattaa olla tärkeämpää määritellä käytettävyyttä yhtäaikaisten käyttäjien määrän avulla.

Kriittisyyttä arvioitaessa on selvitettävä, voidaanko tietojärjestelmä korvata jollain muulla menettelyllä. Käytöstä poissaolo voi olla myös suunniteltua, esimerkiksi huoltokatkokset. Tällöin suunniteltu käytettävyys voi tilapäisesti olla määritellystä luokasta poikkeava.

Tiedon johtamisen luokitus

Tiedon johtamisen kannalta tiedon luokittelun rakenne voisi olla esimerkiksi:

Tietovarantorekisteri tai -kartta on ylimmän tason sisältöalueluokitus (taulukko) : se nimeää tärkeimmät sisältöalueet, niiden yhteydet ja käyttäjäryhmät.

- Sanasto selventää merkityksiä, ja hakusanoja
- Sisältöalueiden sisällä voi olla alaluokkia
- Sisältöluokat voidaan jakaa erilaisiin kriittisyysluokkiin, jotka voivat määritellä tiedon hallinnan prioriteetteja
- Eritasoiset käyttäjäryhmät määritellään luottamuksellisuuden takaamiseksi.

Sisältöluokista on saatavilla eri tavoilla eri tyyppistä tietoa, kuten esim.:

- Toimintatavat
- Toimintaa koskeva tieto: esimerkiksi tavoitteet, mittarit, tulokset.
- Tutkimustieto
- Tuotetieto
- Hanketieto
- Kontaktitieto
- Osaamistieto
- Kokemustieto
- Koulutustieto
- Kysymykset
- Ideat
- Muu hyödylliseksi katsottu tieto.

Nämä tiedot voidaan luokitella eheyden ja käytettävyyden perusteella eri ryhmiin.

Tietojärjestelmien luokitus

Tietojärjestelmiä voidaan luokitella niissä olevien tietojen eheyden, käytettävyyden ja luottamuksellisuuden tai käyttötarkoituksen perusteella esimerkiksi kolmeen luokkaan:

1. Julkiset eli avoimeen käyttöön tarkoitetut sovellukset. Avoin käyttöympäristö on tarkoitettu lähinnä yleisissä tietoverkoissa tarjottaville sovelluksille

2. Käyttöoikeuksin turvatut sovellukset. Sovellusten käyttö on mahdollista vain suojausohjelmiston tunteman käyttäjätunnuksen ja salasanan avulla. Salasanat ja käyttäjätunnukset eivät salaamattomina siirry ei-luotetun verkon yli. Käyttöoikeuksien myöntämiseen liittyvät käytännön toimenpiteet hoidetaan siitä annettujen erillisten ohjeiden mukaisesti.

3. Suljetut sovellukset (tehostettujen turvatoimien sovellukset). Nämä sovellukset on tarkoitettu vain yhden organisaation tai muuten rajoitettuun käyttöön. Sovellukset voi olla eristetty fyysisesti tai loogisesti muusta käyttöympäristöstä. Lisäturvana tarjotaan myös salakirjoitusmahdollisuus.

Sovellusten sijoittamisesta asianomaiseen turvaluokkaan vastaa kunkin sovelluksen vastuuorganisaatio ydinprosessitarkastelun ja tietoturvallisuusanalyysin perusteella. Sovellusten käyttöoikeuksia ja käyttötapoja koskeviin muutoksiin on aina saatava sovelluksen vastuuorganisaation lupa.

Järjestelmien teknisten ominaisuuksien turvaluokitus

Tietoteknisten järjestelmien ja niiden elementtien teknisten ominaisuuksien turvaluokituksessa, tulevaisuudessa myös sovellusten ja palvelujen turvaluokituksessa, käytetään hyväksi tällä hetkellä EU:n tulevassa sertifiointijärjestelmässä käytettävää ITSEC-normistoa.

ITSEC- normisto on tekninen normisto, joka on kehitetty muun muassa useissa spesifikaatioissa esiintyvän USA:n DoD:n “Orange Book’in“ TCSEC-luokituksen pohjalta.

EU:ssa on aloitettu keskustelu siirtymisestä Common Criterian käyttöön. Common Criteria tulee käsittämään teknisten ominaisuuksien lisäksi myös sovellukset ja palvelut. Normistojen hyödyntäminen edellyttää niiden oleellisten ominaisuuksien ja käytännön merkityksen ymmärtämistä. Suomeen pyritään luomaan tällaista tukea antava järjestelmä

TCSEC -luokitus on otettu käyttöön USA:ssa v. 1985 lähinnä sotilaallisiin tarpeisiin ja ITSEC -luokitus on otettu käyttöön Euroopassa v. 1990 sekä julkishallinnon että kaupallisiin tarpeisiin. ITSEC -luokitus eroaa TCSEC:sta eniten siinä, että ITSEC:ssa luokitellaan erikseen tietoturvallisuuden toiminnalliset piirteet ja näiden piirteiden testauksen varmuustasot.

Viimeksi mainitun ominaisuuden vuoksi ITSEC -evaluointi on paljon TCSEC -evaluointia tarkemmin määritelty sekä taustallaan olevan huomattavasti uudemman normiston

vuoksi nykyään selvästi TCSEC -luokitusta luotettavampi.

Vuonna 1993 alkaneessa, monikansallisessa Common Criteria -työssä pyritään kehittämään muun muassa TCSEC:n ja ITSEC:n pohjalta paljon syvemmälle toiminnallisiin ominaisuuksiin = jopa kokonaisiin sovelluksiin ja palveluihin ulottuva luokitusjärjestelmä. Common Criterian keskeisenä tavoitteena on luoda selkeä rakenne ja vaatimukset turvalliselle kansainväliselle tietotekniselle infrastruktuurille.

Näyttää siltä, että Common Criterian mukaisia sovelluksia ja palveluja alkaa tulla käyttöön vuodesta 1999 alkaen. EU-maissa siirryttäneen käyttämään Common Criteriaa ITSEC:n sijasta mahdollisesti vaiheittain vuodesta 2000 alkaen

Toimitilojen luokittelu

Toimitilat jaetaan hierarkisesti vyöhykkeisiin. Vyöhykkeeseen ei sisälly sen sisällä olevat ylemmän turvallisuusluokan vyöhykkeet.

Luokitus määräytyy tapauskohtaisesti toiminnan ja prosessien tärkeysluokitusten tai muiden vastaavien kriteerien avulla.

Käyttäjien luokitus

Oikeudet käyttää tietojärjestelmän tiedostoja ja ohjelmia esim. lukemalla, päivittämällä tai käyttöoikeuksia muuttaen määritetään vastuuorganisaatioiden toimesta.

Käyttäjäprofiilit määritetään ydinprosessien määrityksiin liittyen “rooleina“. Näitä käytetään muun muassa rakenteellisessa ohjeistuksessa sekä mahdollisten henkilökohtaisten käyttöoikeuksien toteutuksessa.

Roolit vaihtelevat organisaatioittain. Kunkin organisaation on määriteltävä tarkoitukseensa sopivat käyttäjäprofiilit. Mahdollisia rooleja voivat olla esimerkiksi:

- järjestelmän tai sovelluksen käyttäjä
- esimies
- tekninen tukihenkilö
- sovellusvastaava
- järjestelmän tai sovelluksen pääkäyttäjä
- järjestelmän tai sovelluksen turvallisuusvastaava
- tietohallintovastaava
- tarkastajat, auditoijat
- järjestelmien toimittajat, kehittäjät, ylläpitäjät ja huoltohenkilöt
- muut ulkopuoliset (sopimuksin tms. määritellyt)

Henkilöitä voidaan luokitella myös esimerkiksi käytettävyyden ja luottamuksellisuuden perusteella.

Jokainen käyttäjä on käyttökohteesta riippuen tunnistettava tai todennettava (identifioitava tai autentikoitava) käyttöoikeusmenettelyjen käytännön toteutuksessa

Luokitusten toteutusvälineitä

Tiedon luokittelun yhteydessä syntyy uutta tietoa, joka kuvaa olemassaolevaa tietoa ja olemassaolevien tietojen välisiä suhteita. Tällaista uutta kuvaavaa tietoa kutsutaan yleisnimellä metadata.

Tiedon luokittelun onnistuneeseen toteuttamiseen tarvitaan siis metadatan hallintaväline. Tällaista hallintavälinettä voidaan lähteä hakemaan ja toteuttamaan esim. seuraavasti:

1. Suunnitellaan tiedon luokittelun tarpeita vastaava tietomalli tietokantaan ja rakennetaan sovellus, jolla tätä tietomallia hallitaan.

2. Tiedon luokittelu-projektin ongelmakenttä on hyvin samanlainen yleisten datawarehouse-projektien ongelmakenttien kanssa. Jotkin datawarehouse-ratkaisut sopivat ongelmaan tyydyttävällä tavalla.

3. Markkinoille on ilmestynyt välineitä, joilla voidaan hallita datawarehouse-projekteissa syntyvää metadataa. Näillä voidaan inventoida informaatio, joka sijaitsee tietokannoissa, erilaisissa dokumenteissa ja muodoissa tai Internetissä yrityksen sisällä tai ulkona. Niillä voidaan luokitella informaatiota erilaisiin tarpeisiin ja tietolähteen tai käytön mukaan.

4. Perinteisesti tietojärjestelmien mallintamiseen, suunnitteluun, toteuttamiseen ja edelleen kehittämiseen liittyvää metadataa on hallittu erilaisilla CASE-välineillä. Niitä ei kuitenkaan ole suuniteltu tiedon luokitteluprojektin tarvitsemien tiedon luokittelusta syntyvien tietojen tallentamiseen. Tämä koskee kaikkia perinteisiä CASE-välineitä, koska niiden tiedon kuvaamiseen käyttämä malli, metamalli, on kiinteä, eikä siihen ole helppo lisätä uusia piirteitä.

5. On olemassa välineitä, joilla voidaan mallintaa metamalleja ja jotka siis tuottavat ja käsittelevät meta-metadataa ja perustuvat **GOPRR** (Graph, Object, Property, Role, Relationship) -malliin. Tällaisella työvälineellä voidaan luoda tiedon luokitteluun räätälöity metamalli (ja ylläpitää sitä).

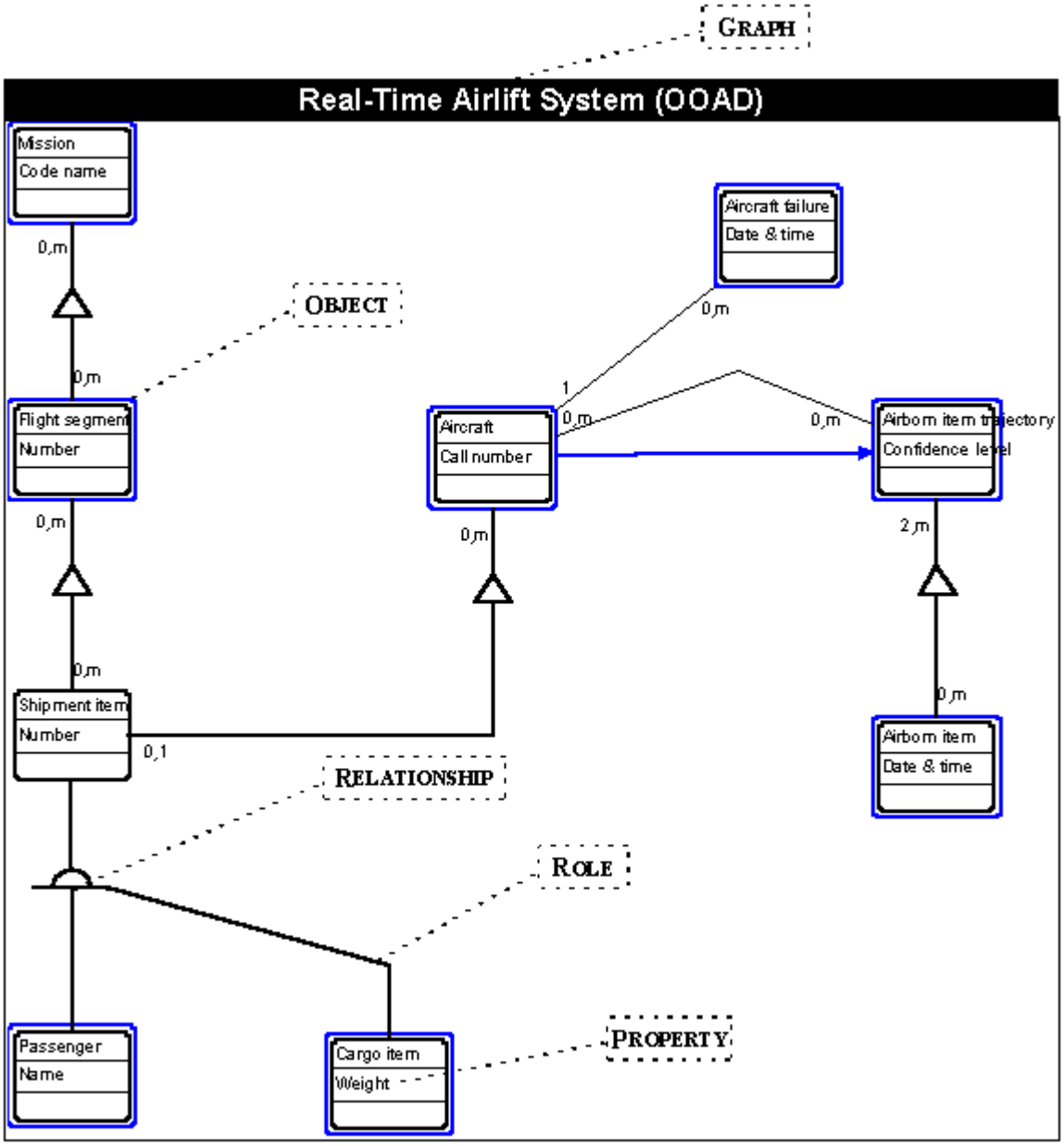
Väline tarjoaa usealla alustalla toimivan, useita menetelmiä tukevan, usean käyttäjän integroidun työkalujoukon. Työkalut yhdistää oliorepositori ja niillä on samanlainen käyttöliittymä ja toiminnallisuus käytetystä menetelmästä riippumatta.

Tietoa voidaan kuvata kolmella erityyppisellä välineellä, kaavio-, matriisi- ja/tai taulueditorilla. Repositorin sisällön tutkimiseen ja editointiin väline tarjoaa tyyppi- ja graafiselaimen. Lisäksi se sisältää raporttiselaimen, jota voi käyttää raporttien, tarkistusten ja ohjelmakoodin tuottamiseen.

Edellä olevan lisäksi metamallinnusväline sisältää työkalun, jolla voi tehdä omia menetelmiä, jotka voi ottaa käyttöön tiedon kuvaamisessa standardimenetelmien lisäksi. Tämä piirre tekee kyseisen välineen varsin houkuttelevaksi: Suunnitellaan menetelmä, jolla tiedon luokittelu voidaan tehdä halutulla tavalla!

Tietojen ja niihin liittyvien luokittelujen kuvaamisen lisäksi väline mahdollistaa mallien tarkistamisen sekä kyselyt mallitietoihin. Tällöin esimerkiksi tietojen yhdisteltävyyttä voidaan tarkistaa esim. luottamuksellisuuden tai niiden laadun kannalta.

Esimerkki GOPRR-mallin mukaisista kuvausperiaatteista on esitetty kuvassa 1.



KUVA 1 GOPRR concepts illustrated by a graph and its contents

Luokitusprosessi

Jotta turvallisuuden ja erityisesti tietoturvallisuuden kehittämiseen tähtäävät toimenpiteet voidaan kohdistaa optimaalisesti on mm. tiedot, tietojärjestelmät, tilat ja käyttäjät luokiteltava, ja mieluiten jo järjestelmien kehitysvaiheessa. Tätä työtä ei yleisesti ole tehty ja siksi siitä seuraakin oma ylimääräinen kehitysprosessinsa. Usein rajalliset tietoturvallisuustoimenpiteet ja resurssit voidaan luokitusten avulla kohdentaa tärkeimpiin kohteisiin eli panostaa oikein. Tällöin niiden vaikutukset ovat myös tehokkaimmat.

Luokitusprosessi koostuu omana kertaluonteisena kehitysprosessinaan esim. pilotointiprojektista, luokitteluperiaatteiden määrittelemisestä ja varsinaisesta luokitustyöstä, sekä jatkuvana prosessina soveltamisesta systeemityöhön tietojärjestelmien elinjakson eri vaiheissa osana tietoturvallisuuden kehittämisprosessia.

Tietoturvallisuustehtäviä tietojärjestelmien elinjakson eri vaiheissa käsitellään toisaalla tässä julkaisussa.

Lähteet, kirjallisuutta

Tietoaineiston luokitus ja käsittely, raportti 29.5.1995, Tietoaineiston luokitustyöryhmä (TILU), Valtiovarainministeriön työryhmämuistioita 1995:6 (http://www.vn.fi/vm/suomi/muuta/vahti/tilurap2.htm)

DoD Directive 5200.1, "DoD Information Security Program," December 13, 1996.

Tiedon luokituksen esiselvitys, Pääesikunta 1998

Appendix 1 in Kelly, S., "Towards a Comprehensive MetaCASE and CAME Environment: Conceptual, Architectural, Functional and Usability Advances in MetaEdit+", Ph.D. Thesis, Jyväskylä University, 1997

Valtiohallinnon tietoturvallisuuskäsitteistö, Valtionhallinnon tietoturvallisuuden johtoryhmä 18.4.1997, http://www.vn.fi/vm/suomi/muuta/vahti/sanasto.htm

Kirjoittaja

Aarno Kansikas toimii johdon konsulttina ICL Konsultoinnissa tärkeimpänä erityisosaamisalueenaan tietoturvallisuuden kehittämisprosessi. Hän on myös Tietoturva ry:n hallituksen jäsen.

puh. 09-567 3450
aarno.kansikas@icl.fi

Tietoturvallisuus tietojärjestelmän elinkaaren eri vaiheissa

Hellevi Huhanantti,
Järjestelmäpäällikkö,
Tietoleonia Oy

Tässä artikkelissa tarkastelemme tietojärjestelmän turvavaatimuksia tietojärjestelmän elinkaaren aikana. Artikkeli pohjautuu kirjoittajan omaan kokemukseen sekä Hetkyn tietoturvakerhon raporttiin “Sovelluskehitys ja tietoturvallisuus“.

Riippumatta siitä millä menetelmällä tietojärjestelmä on kehitetty on samat turvatoimet otettava huomioon. Tässä kuvaamamme vaihejakomallin vaiheiden tehtävät myös turvatehtävtät voidaan suorittaa eri vaiheissa menetelmästä riippuen.

Tietojärjestelmä kehitetään moduuleina tai komponentteina, jotka sitten istutetaan sovelluskehikkoon. Kehittämisen tavoitteena on saada aikaan halutut vaikutukset tuottava toiminta. Tietojärjestelmällä tuetaan liiketoimintaa hoitamalla osa sen vaatimasta tietojenkäsittelystä.

Tietojärjestelmän elinkaarimallin vaiheet ovat seuraavat:

- esitutkimus
- määrittely
- suunnittelu
- toteutus
- käyttöönotto
- ylläpito
- käytöstäpoisto

Tässä artikkelissa käytetään seuraavia turvaamiseen liittyviä peruskäsitteitä:

- Turvaamisella tarkoitetaan toimintaa, jolla riskejä pyritään minimoimaan.
- Tietojenkäsittelyn turvaamisella (tietoturvalla) pyritään ensisijaisesti estämään vahinkoja, jotka aiheutuvat toiminnalle tietojen tai tietojenkäsittelyn riskeistä.
- Tietoriskejä ovat sellaiset tietoihin tai niiden käsittelyyn kohdistuvat uhat, jotka aiheuttavat haittaa. Tietoriskejä voivat aiheuttaa mm. tahalliset ja tahattomat inhimilliset teot, ohjelmistohäiriöt, laiteviat sekä luonnontapahtumat.
- Turvatoimet ovat tehtäviä tai toimintaa, joilla mm.
  - estetään vahinkojen aiheutuminen
  - poistetaan vaaran aiheuttajat
  - paljastetaan epäsuotuisat tapahtumat
  - rajoitetaan epäsuotuisten tapahtumien vaikutuksia
  - toivutaan epätavallisten tapahtumien vaikutuksista
- Turvatoimissa käytetään turvakeinoja, joista etenkin sovelluskontrolleja.

Luotettava ja turvallinen toiminta on yritykselle laatua ja kilpailuetua. Tietojärjestelmät ovat nykyisin oleellinen osa yrityksen liiketoimintaa. Siksi tietojärjestelmien kehittämisessä on osattava arvioida liiketoiminnan tietojenkäsittelyyn kohdistuvat riskit sekä osattava ottaa huomioon turvavaatimukset.

Tietojärjestelmien omistajien ja käyttäjien tarpeet tulee esittää vaatimuksina, jotta järjestelmä voidaan toteuttaa tarkoituksenmukaisesti. Tärkeää on, että koko tietojärjestelmällä sekä kullakin tiedolla on yksikäsitteinen omistaja, joka määrittelee turvavaatimukset ja vastaa tietoturvan toteuttamisesta sekä sen noudattamisesta ja valvonnasta.

Tietojärjestelmän kehittämisestä saatu kokemus osoittaa, että vieläkin turvavaatimukset määritellään, suunnitellaan ja toteutetaan kokonaisuuden kannalta liian myöhään. Turvakeinot oletetaan voivan lisätä tietojärjestelmään vasta järjestelmän käyttöönottovaiheessa. Tietoturvakeinoja ei suinkaan aina voi ostaa valmiina paketteina ohjelmistotoimittajilta, vaan tietoturvakeinot on suunniteltava tietojärjestelmän kuten muukin tietojärjestelmän toiminta kehittämisen eri vaiheissa. Jos turvavaatimusten toteuttaminen jätetään esimerkiksi käyttöönottovaiheeseen on se vaikeaa, aikaa vievää ja kallista. Turvavaatimukset saattavat jäädä myös kokonaan toteuttamatta. Tietojärjestelmän kehittäjien on siten osattava oikein vaiheistettuna arvioida liiketoimintaan sekä tietojärjestelmään ja sen kehittämiseen liittyviä uhkia sekä suunniteltava määritellyt vaatimukset toteuttavat turvatoimet ja niihin liittyvät turvakeinot ja kontrollit. Tietojärjestelmän turvavaatimusten ja -keinojen suunnittelun vastuu on tietojärjestelmien suunnittelijoilla sekä järjestelmän omistajalla. Tietojärjestelmien suunnittelussa on syytä käyttää tietoturva-asiantuntijoita tietoturvavaatimuksia ja -keinoja kartoitettaessa.

Tietojärjestelmät ovat laajentuneet myös yritysten välisten työketjujen ja tiedonsiirron hoitamiseen. Tietojärjestelmät yhä enemmän välittävät ja käyttävät samoja tietoja yritysten sisällä ja yritysten välillä. Tietoturvan merkitys korostuu siten entisestään. Samoin korostuu tietojen omistajien vastuu tiedoista ja turvaratkaisuista. Keskeisiä vaatimuksia ovat mm. että siirrettävien tietojen oikeellisuus, asiattomien pääsy tietoihin , tietojen luottamuksellisuus ja liiketoiminnan häiriöiden jatkuminen..

Myös tietojenkäsittely-ympäristöt monipuolistuvat, mikä aiheuttaa turvatoimien kehittämiseen uusia työta-

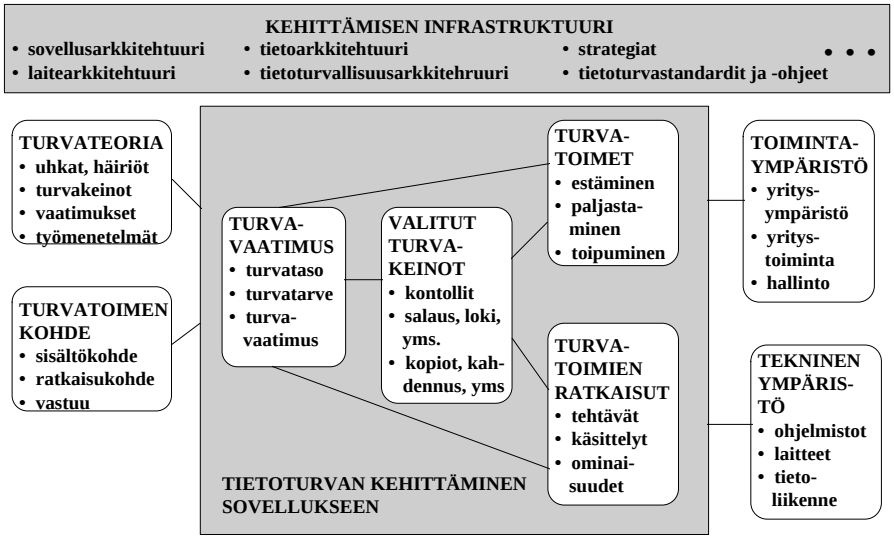
poja. Tietojenkäsittelyn uhat ovat samoja ratkaisuista riippumatta. Turvatoimet toteutetaan teknisesti eri tavoin. Sovellusten kehittäjät valitsevat olemassaolevista, lukuisista turvatoimista sovelluksissa tarvittavat ominaisuudet. Hajautettujen tietojärjestelmien kehittämistyö ei aina ole kovin muodollista ja näinollen myös turvatoimet eivät tule riittävästi huomioiduiksi. Tällöin turvatoimien toteutus jää usein tietojärjestelmän omistajien ja käyttäjien aktiivisuuden varaan.

Muuttuneet tarpeet, ympäristöt ja vastuut edellyttävät yrityksen tietoturvaperiaatteiden lisäksi uusia ohjeita tietoturvan suunnitteluun ja toteuttamiseen sovelluskehityksen osana. Ohjeen tulee antaa tukea tietojärjestelmien sekä omistajille että kehittäjille. Tietojärjestelmän kehittämistä ohjaa tietoturvakehikko, joka koostuu tietoturvapolitiikoista, -arkkitehtuureista, -standardeista ja -ohjeista.

Valmisohjelman hankinnassa painottuu tarpeiden ja vaatimusten määrittely. Eri ohjelmistoja arvioidaan määrityksiä vastaan myös tietoturvan kannalta. Valmisohjelmistot saattavat edellyttää käyttöympäristöön tietoturvan muutoksia ja sovittamista. Määritykset saattavat aiheuttaa myös valmisohjelmiston täydentämistä tietoturvan osalta.

Tietojärjestelmän **käytössä** korostuvat järjestelmän käyttäjät ja heidän toimintansa sekä tietojärjestelmän osien käyttö toiminnan tukena. Käyttöön kuuluu myös seuranta, joka on suunniteltava ennen käyttöönottoa. **Ylläpito** pitää sisällään tietojärjestelmän toimivuuden säilyttämisen ja virheiden korjauksen. Tietojärjestelmän **käytöstä poistoon** liittyy paljon turvallisuuteen kuuluvia tehtäviä.

Seuraavassa kuvassa on esitetty tietoturvan kehittämiseen sovelluksessa liittyvät peruskäsitteet ja niiden väliset suhteet.



Turvavaatimukset esitetään alussa uhkina ja tarpeina, jotka sitten tarkentuvat hyväksytyiksi vaatimuksiksi. Vaatimusten määrittelyssä käytetään apuna turvaamisen teoriaa eli mm. uhkaluetteloita, vaatimusten jäsentelyjä, riskianalyysin suoritusohjeita.

Vaatimusten perusteella valitaan **turvatoimet**, jotka liittyvät häiriöiden ja poikkeustilanteiden estämiseen, paljastamiseen ja käsittelemiseen sekä häiriöistä toipumiseen. Turvatoimet liittyvät sovelluksen sisältö- ja ratkaisukohteisiin.

Turvatoimissa käytetään hyväksi erilaisia **turvakeinoja**, jotka voivat olla periaatteita tai konkreettisia tuotteita. Periaatteellisiin turvakeinoihin kuuluvat mm. kontrollit, lokit, salausmenettelyt, kopiointi. Tuotteita ovat mm. salausohjelmisto, varmuuskopiointimenettely. Turvakeinojen valintaan vaikuttavat turvavaatimukset sekä käytettävissä olevat turvaratkaisut.

Turvatoimien ratkaisut ovat ohjelmallisia käsittelyjä, valittuja teknisten ympäristöjen ominaisuuksia ja käyttäjän toimintaa. Tehtäviä ovat mm. ohjaus-, suoritus-, seuranta-, palautus- ja tukitehtävät. Teknisen ympäristön ominaisuudet liittyvät mm. käyttöjärjestelmään, turva-, tiedonhallinta- ja tietoliikenneohjelmistoihin sekä hallintakäytäntöihin.

Toiminta- ja tekninen ympäristö asettavat turvavaatimuksia kehitettävälle toiminnalle. Kehittämisen aikana tehdyt päätökset ja ratkaisut asettavat ympäristölle turvaamisen **muutosvaatimuksia**, joiden toteuttaminen on usein sovelluksen käyttöönoton edellytys. Muutosvaatimukset voivat kohdistua mm. henkilöstöhallintoon, yrityksen ulkopuolelle, kulun- ja kuljetuksenvalvontaan, palo- ja rikossuojeluun, toimintaohjeisiin, laadunohjaukseen sekä laitteiden ja tietoliikenteen valvontaan ja kunnossapitoon

Seuraavassa taulukossa on esitetty karkea luettelo turvatehtävistä ja turvaamisen päätuloksista tietojärjestelmän elinkaarimallin eri vaiheissa. Luettelo on viitteellinen.

VAIHE JA SEN TARKOITUS	TURVAN KEHITTÄMISTEHTÄVÄT KYSEISESSÄ VAIHEESSA	TURVATEHTÄVÄN PÄÄTULOKSET
ESITUTKIMUS Päämääränä on antaa perusteltu ehdotus kehittämisestä ja sen vaikutuksista	TURVATASON VALINTA • Määritetään turvatarpeet • Tehdään alustava riskianalyysi • Määritetään turvatoimintojen puitteet	• Turvatarpeet – sovelluksen/tietojen kriittisyys – turvallisuuden päämäärät – turvakontrollien kuormitusvaikutus • Toiminnan riskiluettelot – uhkat/riskit – tekniikka jne • Arvio turvatoimien hyödyistä/kustannuksista • Turvatoimien puitteet – oleelliset turvatoimet
MÄÄRITTELY Tietojärjestelmän yksityiskohtaiset vaatimukset, tieto- sekä toimintosisältö sekä rakenne määritellään.	TURVAVAATIMUSTEN MÄÄRITTELY • Määritetään turvavaatimukset • Tarkennetaan riskianalyysiä • Tehdään jatkuvuussuunnitelma • Määritellään alustava turvatoimien testaus • Sisällytetään turvavaatimukset toteutusstrategiaan, sopimuksiin • Sisällytetään turvatoimet perustoimintoihin	• Tarkennetut turvavaatimukset – uudet uhkat/riskit – järjestelmään sijoitetut turvavaatimukset • Jatkuvuussuunnitelma – toipumissuunnitelma – käyttäjän toimintojen suunnitelma – manuaalitoiminnot • Alustava turvatoimien testaussuunnitelma – tarkennetut turvavaatimukset – testausaikataulu ja resurssit – arviointiperusteet • Tietoturvavaatimukset sopimuksissa • Toimintokohtaiset turvavaatimukset
SUUNNITTELU Sovelluksen toiminta- ja ratkaisuvaihtoehdot hahmotellaan ja valitusta ratkaisusta suunnitellaan yksityiskohtaiset työnkulut, käyttäjän toiminta sekä ohjelmisto- ja tietokantaratkaisut	TURVATOIMIEN SUUNNITTELU • Suunnitellaan sovelluksen turvatoimet • Tarkennetaan turvatoimien testaussuunnitelmaa • Suunnitellaan turvatoimet perustoimintoihin	• Turvatoimien suunnitelmat – järjestelmät ja liittymät – ohjelmat, tietokannat, tietoliikenneverkot jne • Päivitetty turvatoimien testaussuunnitelma – normaali toiminnassa – epätavallisissa tilanteissa • Turvatoimet perustoiminnoissa
TOTEUTUS Toteutetaan ja testataan tekniset ratkaisut ja ohjelmat sekä laaditaan käyttöohjeet	TURVATOIMIEN TOTEUTUS • Toteutetaan suunnitellut turvatoimet • Testataan turvatoimet ja kontorollit • Sisällytetään turvatoimet varsinaisiin toimintoihin	• Turvatoimien testatut ohjelmamoduulit • Testattu tietojärjestelmä • Turvatoimien testauspöytäkirjat • Turvatoimien käyttöohjeet

VAIHE JA SEN TARKOITUS	TURVAN KEHITTÄMISTEHTÄVÄT KYSEISESSÄ VAIHEESSA	TURVATEHTÄVÄN PÄÄTULOKSET
KÄYTTÖÖNOTTO Systeemi- ja käyttöönotto-testauksien hyväksymisen jälkeen toiminta siirretään käyttäjien ja tukiorganisaatioiden vastuulle	TURVATOIMIEN KÄYTTÖÖNOTTO • Suoritetaan turvatoimien käyttöönottotestaus • Suoritetaan testaus integroidussa ympäristössä • Suoritetaan hyväksyntätestaus • Tarkennetaan turvakuvauksia	• Turvatoimien testauspöytäkirjat • Turvattu tietojärjestelmä • Koulutetut käyttäjät • Turvaohjeistot • Turvakuvaus • Arkistoitu aineisto
YLLÄPITO Käyttöönoton jälkeen järjestelmään toteutetaan toimintaympäristön muutoksista tai muista syistä tarvittavat pienehköt muutokset.	TURVATOIMIEN YLLÄPITO • Suunnnitellaan ja toteutetaan järjestelmän muutosten turvatoimiin aiheuttamat muutokset • Testataan ja otetaan käyttöön turvatoimien muutokset. Käyttäjille koulutus muutoksista.	• Turvatoimien muutosten vaatimukset ja määrittelyt • Testatut turvatoimien muutokset • Turvatoimien testauspöytäkirjat • Turvatoimien käyttöohjeet • Muutoksiin koulutetut käyttäjät
JÄRJESTELMÄN VERSION VAIHTO Toimintaympäristössä tapahtuu merkittäviä muutoksia tai tekniset syyt (esimerkiksi käyttöympäristön vaihto) pakottavat tekemään järjestelmään pienimuotoista ylläpitoa laajempia muutoksia	TURVATOIMIEN MUUTOKSET • Turvatoimien, kuten muun kehittämisen osalta käydään läpi edellä kuvatut vaiheet • Suunnitellaan ja toteutetaan turvatoimien muutokset • Varmistetaan turvallisuus tiedonsiirrossa väistyvästä järjestelmästä /versiosta uuteen ympäristöön • Väistyvän järjestelmän tietojen, ohjelmien ja dokumentaation arkistointi / hävittäminen • käyttövaltuuksiin tehdään järjestelmämuutosten edellyttämät muutokset/tarkennukset	• Uuden järjestelmän/version osalta edellisissä vaiheissa kuvatut tulokset, joiden lisäksi – Kuvaukset turvatoimien muutoksista ja muutosten toteutuksesta – Kuvaukset vanhasta järejstelmästä/versiosta uuteen tehdyn tietojen siirron turvaamismenettelyistä – kuvaus käyttövaltuuksien muutoksista – Tiedon siirron pöytäkirja/loki – Järjestelmän ja turvatoimien muutoksiin koulutetut käyttäjät • Väistyvän järjestelmän/version osalta – Kuvaus tietojen, ohjelmien sekä dokumentaation arkistoinnista ja hävittämisestä – Loki tehdyistä toimenpiteistä
KÄYTÖSTÄ POISTO Käytöstä poistettavan järjestelmän toiminnot ajetaan alas hallitusti	KÄYTÖSTÄ POISTON TURVATOIMET • Suunnitellaan ja toteutetaan turvatoimien muutokset niihin järjestelmiin, joilla on liittymiä poistettavaan järjestelmään • Poistuva järjestelmä ajetaan alas hallitusti • Dokumentaatio, ohjelmat ja tiedot arkistoidaan tarvittavin osin, muut hävitetään • Käyttövaltuuksiin tehdään järjestelmän poiston edellyttämät muutokset	• Tarvittavat muutokset järjestelmissä, joilla on liittymiä poistettavaan järjestelmään • Kuvaus poistettavan järjestelmän tietojen sekä dokumentaation arkistoinnista ja hävittämisestä • Kuvaus käyttövaltuuksien poistamismenettelyistä • Asianmukaisesti arkistoidut/hävitetyt poistettavan järjestelmän dokumentaatio ja tiedot • Pöytäkirja/loki tehdyistä toimenpiteistä

Järjestelmän esitutkimus

Hellevi Huhanantti,
Järjestelmäpäällikkö,
Tietoleonia Oy

Esitutkimusvaihe valmistelee tietojärjestelmäprojektin. Esitutkimuksen lähtökohtana on kehittämistarve ja lopputuloksena tietojärjestelmän kehittämisehdotus tavoitteineen, rajauksineen, perusteluineen ja investointilaskelmineen.

Vaiheen tarkoitus ja toiminnot

Päämääränä on antaa perusteltu ehdotus tietojärjestelmän kehittämisestä ja sen vaikutuksista.

Tärkeimmät turvatehtävät esitutkimusvaiheessa

TURVATOIMIEN ESITUTKIMUS

- Määritetään turvatarpeet
- Tehdään alustava riskianalyysi
- Määritetään turvatoimintojen puitteet

Esitutkimusvaiheen jälkeen on tietojärjestelmähankkeen omistajan kyettävä päättämään onko tietojärjestelmän kehittäminen kannattava hanke arvioimalla hyötyjä ja kustannuksia. Päätöstä varten tarvitaan riittävän kattava liiketoiminta-alueen toiminnan riskien kartoitus.

Esitutkimuksessa tärkein tietoturvatehtävä on kartoittaa mitä menetyksiä liiketoiminnalle aiheutuu jos tietoturvallisuus pettää. Toinen tärkeä tämän vaiheen turvatehtävä on tietojärjestelmän, käsiteltävien tietojen, tietojenkäsittely-ympäristön ja joskus jopa henkilöstönkin alustavan tietoturvallisuusluokan määrittäminen. Tietojärjestelmän tietoturvallisuusluokitus määrittää minkä tasoiset kontrollit ovat tarpeen. Tässä lehdessä on toisaalla oma artikkeli aiheesta tietoturvallisuusluokitukset.

Riskikartoituksen perusteella määritetään mitkä ovat tärkeimmät tietoturvatoimet. Luokituksen perusteella arvioidaan mitä ja minkä tasoiset kontrollit ovat tarpeen, jotta turvavaatimukset tulevat toteutetuksi.

Riskikartoituksen ja turvavaatimusten avulla arvioidaan vaadittavien turvatoimien kustannus-, hyöty- sekä kuormitusvaikutuksia. Turvatoimia arvioitaessa on huomioitava myös turvatoimissa käytettävä tekniikka.

Turvatoimien jatkokehittämisen kannalta on tärkeä tietää, onko tarvittava tekniikka jo aikaisemmin yrityksessä otettu käyttöön vai joudutaanko se rakentamaan tietojärjestelmän kehittämishankkeen yhteydessä. Turvatoimien kustannuksiin vaikuttaa oleellisesti mitä valmiita ratkaisuja on yrityksessä jo kehitetty tietojärjestelmien turvaamiseksi.

Tietojärjestelmien turvatoimille on olemassa useissa yrityksissä jo paljon valmiita ratkaisuja, joita voidaan hyödyntää sellaisenaan tai pienehköllä työmäärällä. Aina ei kuitenkaan ole valmista turvaamiskeinoa valmiina ja yhä useammin tietojärjestelmähankkeissa rakennetaankin uutta infrastruktuuria. Rakennettaessa uutta infrastruktuuria onkin otettava huomioon, että kehittämisen riskit, toteutusaika ja kustannukset kasvavat.

Esitutkimusvaiheen aikana kartoitetaan oleellisimmat turvavaatimukset ja -toimet ja arvioidaan niiden hyödyt sekä kustannus- ja kuormitusvaikutukset.

Turvatehtävien päätulokset esitutkimusvaiheessa

- *Turvatarpeet*
  - *Tietojärjestelmän / tietojen kriittisyysluokitus*
  - *turvallisuuden päämäärät*
  - *turvakontrollien kuormitusvaikutus*
- *Toiminnan riskiluettelot*
  - *uhkat / riskit*
  - *tekniikka*
  - *...*
- *Arvio turvatoimien hyödyistä / kustannuksista*
- *Turvatoimien puitteet*
  - *oleelliset turvatoimet*

Järjestelmän määrittely

Hellevi Huhanantti,
Järjestelmäpäällikkö,
Tietoleonia Oy

Määrittelyvaiheessa kartoitetaan tietojärjestelmälle asetettavat vaatimukset sekä määritellään tietojärjestelmän rakenne. Tässä vaiheessa myös valmistellaan tietojärjestelmän suunnittelun ja toteutuksen tarjouspyynnöt tietojärjestelmän toimittajille.

Vaiheen tarkoitus ja toiminnot

Tietojärjestelmän yksityiskohtaiset vaatimukset, tieto- sekä toimintosisältö ja rakenne määritellään.

Tärkeimmät turvatehtävät määrittelyvaiheessa

TURVATOIMIEN MÄÄRITTELY

- Määritetään turvavaatimukset
- Tarkennetaan riskianalyysiä
- Tehdään jatkuvuussuunnitelma
- Määritellään alustava turvatoimien testaus
- Sisällytetään turvavaatimukset toteutusstrategiaan, sopimuksiin
- Sisällytetään turvatoimet perustoimintoihin

Kun esitutkimusvaiheen jälkeen on tehty kehittämispäätös, seuraa tietojärjestelmän vaatimusten määrittely. Määrittelyvaiheessa tarkentuvat riski/uhkaluettelot sekä tietoturvavaatimukset. Tietoturvavaatimusten pohjalta määritellään tarkennetut turvatoimet. Tärkeimpiä turvavaatimuksia ovat esimerkiksi

- toiminta- ja yritysympäristön vaatimukset kuten lait, säädökset, yrityksen turvapolitiikat, jne
- fyysisen ympäristön vaikutukset, esimerkiksi olemassaolevat fyysiset turvaamiskeinot kuten kulunvalvonta, paloturvallisuus jne
- tietoteknisen ympäristön vaatimukset, esimerkiksi laite- ja sovellusarkkitehtuurit, sekä turva-arkkitehtuurit ja turvamenettelyt
- käyttö- ja kehitysympäristön turvavaatimuksia ovat esimerkiksi kehitys- ja testausympäristöt, tuotantoympäristö, kehittämismenettelyt, tuotantoonsiirto- ja varmistusmenettelyt, toipumissuunnitelmat sekä muutostenhallinta.

Yrityksissä on olemassa paljon jo tehtyjä tietoturvapolitiikoita sekä tietoturva-arkkitehtuureja ja sovittuja varmistus- ja toipumismenettelyjä, jotka luovat yleisen perustan turvatoimille. Jos tietojärjestelmän kehittämishankeessa rakennetaan uutta teknologiaa hyödyntävää järjestelmää niin silloin ei kaikkiin turvavaatimuksiin löydy ratkaisua olemassaolevista arkkitehtuureista ja politiikoista, vaan on samalla rakennettava turva-arkkitehtuuria. Nykyisin tämän tyyppinen tilanne onkin varsin usein tietojärjestelmähankkeissa, koska uusia arkkitehtuuriratkaisuja ei enää rakenneta erillisinä hankkeina.

Edellä lueteltujen lisäksi tärkeitä turvavaatimuksia ovat erilaiset sovelluskontrollit kuten pääsynvalvonta, tietojen luottamuksellisuuden varmistaminen sekä tietojen eheyskontrollit.. Turvavaatimuksia ovat edellisten lisäksi myös tietojärjestelmien tietojen ja käsittelyn jäljitettävyys.

Määrittelyvaiheessa tehdään jo alustava turvatoimien testaussuunnitelma resurssitarpeineen sekä arviointikriteereineen.

Jos järjestelmä ostetaan ulkopuoliselta toimittajalta on tarjouspyyntöön liitettävään tietojärjestelmäkuvaukseen syytä liittää myös määrittelyvaiheesta syntynyt turvavaatimusten kuvaus. Tällöin tarjousta käsiteltäessä myös vaadittavat turvatoimien suunnittelu- ja toteutustarpeet tulee huomioiduksi työmääriä ja kustannuksia arvioitaessa. Usein vieläkin tietoturvallisuusvaatimuksien kuvaukset puuttuvat tietojärjestelmien tarjouspyynnöistä. Tästä syystä yhä edelleen käy niin, että tietoturvavaatimuksien kehittäminen alkaa vasta suunnittelutai jopa toteutusvaiheessa. Näin menetellen tietoturvaratkaisuista tulee usein hankalia ja kalliita.

Turvatehtävien päätulokset

- *Tarkennetut turvavaatimukset*
  - *uudet uhkat/riskit*
  - *järjestelmään sijoitetut turvavaatimukset*
- *Jatkuvuussuunnitelma*
  - *toipumissuunnitelma*
  - *käyttäjän toimintojen suunnitelma*
  - *manuaalitoiminnot*
- *Alustava turvatoimien testaussuunnitelma*
  - *tarkennetut turvavaatimukset*
  - *testausaikataulu ja resurssit*
  - *arviointiperusteet*
- *Tietoturvavaatimukset sopimuksissa*
- *Toimintokohtaiset turvavaatimukset*

Järjestelmän suunnittelu

Hellevi Huhanantti,
Järjestelmäpäällikkö,
Tietoleonia Oy

Suunnitteluvaiheessa suunnitellaan käyttäjätehtävät ja käyttöliittymät, tulosteet, tietokannat sekä kontrollit.

Vaiheen tarkoitus ja toiminnot

Sovelluksen toiminta- ja ratkaisuvaihtoehdot hahmotellaan ja valitusta ratkaisusta suunnitellaan yksityiskohtaiset työnkulut, käyttäjän toiminta sekä ohjelmisto- ja tietokantaratkaisut.

Tärkeimmät turvatehtävät suunnitteluvaiheessa

TURVATOIMIEN SUUNNITTELU
- Suunnitellaan sovelluksen turvatoimet
- Tarkennetaan turvatoimien testaussuunnitelmaa
- Suunnitellaan turvatoimet perustoimintoihin

Suunnitteluvaiheessa tarkennetaan toteutettavaksi valittuja turvatoimia. Suunnitteluvaiheessa turvatoimet jakaantuvat esimerkiksi sen mukaan onko turvavaatimukselle olemassa valmiit ratkaisut vai onko turvatoimille rakennettava ohjelmistoa tai hankittava esimerkiksi uusia laitteita.

Jos valmiit ratkaisut ovat olemassa ei tarvita erillistä teknistä suunnittelua. Valmiita ratkaisuja voivat olla esimerkiksi salausohjelmiston käyttö tai valmiit syöttökontrollimoduulit jne. Ellei turvatoimen toteuttamiseen ole olemassa valmista ratkaisua, tehdään turvatoimien suunnittelu. Turvatoimet tarkentuvat esimerkiksi tiedon eheystarkistukseksi, syöttökontrollimoduuleiksi tai tietokannan eheyden tarkistusmenettelyksi, luottamuksellisten tietojen salausohjelmasuunnitelmiksi jne.

Suunnitteluvaiheessa suunnitellaan käyttäjän tehtävät ja yksi tärkeitä turvatehtäviä on suunnitella käyttäjien käyttövaltuudet. Käyttövaltuudet määritetään siten, että käyttäjällä on työtehtävien mukaiset käyttövaltuudet. Käyttövaltuuksia suunniteltaessa on muistettava myös järjestelmän valvonnan tarpeet eli on suunniteltava käyttäjäryhmiä, joilla on tarvittavat oikeudet valvoa tietojärjestelmää eri tavoin.

Suunnitteluvaiheessa tarkennetaan testaussuunnitelmaa. Tässä vaiheessa ovat tarkentunut toteutuksen työmäärä- ja aikatauluarvio sekä testattavat kohteet ja voidaankin suunnitella testausympäristö ja testitapahtumat sekä varata testausresurssit. Testaustapahtumien tulee kattaa sekä epätavalliset että normaalit tilanteet.

Suunnitteluvaiheessa tarkennetaan jatkuvuussuunnitelmaa sekä suunnitellaan toiminnot, joilla selvitään häiriötilanteiden yli.

Virhetilanteiden hallinnan suunnittelu on myös tärkeä turvatoiminto ohjelmistojen suunnitteluvaiheessa. Virhetilanteiden ilmoitukset tulee suunnitella huolella, jotta käyttäjä ymmärtää myös mistä on kysymys. Suunnitteluvaiheen tärkeimmät turvatehtävät ovat ohjelmiin suunniteltavat turvakontrollit sekä testaussuunnitelman teko ja käyttäjän tehtäviin liittyvät kontrollit.

Tässä artikkelissa en ole tarkastellut lainkaan laadun varmistamista, mikä on oleellinen osa tietojärjestelmäprosessia ja takaa, että tietojärjestelmä tulee vastaamaan sille asetettuja vaatimuksia.

Turvatehtävien päätulokset

- *Turvatoimine suunnitelmat*
  - *järjestelmät ja liittymät*
  - *ohjelmat, tietokannat, tietoliikenneverkot jne.*
- *Päivitetty turvatoimien testaussuunnitelma*
  - *normaalitoiminnassa*
  - *epätavallisissa tilanteissa*
- *Turvatoimet perustoiminnoissa*

Järjestelmän toteutus

Helvi Salminen,
Tietoturva-asiantuntija,
Setec Oy

Toteutusvaiheessa vaatimukset, määritykset ja suunnitelmat jalostuvat ohjelmiksi, joiden toimivuus testataan kehitysympäristössä.. Laadukas toetutustyö on edellytys toimivalle ja turvalliselle järjestelmälle.

Vaiheen tarkoitus ja toiminnot

Toteutetaan ja testataan tekniset ratkaisut ja ohjelmat sekä laaditaan käyttöohjeet. Toteutukseen sisältyvät myös turvatoimet.

Pohja onnistuneelle toteutusvaiheelle on luotu sitä edeltävissä suunnitteluvaiheissa. Hyvin ja huolella tehty määritys- ja suunnitteluvaihe vähentävät toteutusvaiheen työmäärää.

Toteutusvaihe on paljolti raakaa työtä, jossa tehdään ja testataan ohjelmia aiemmissa vaiheissa syntyneiden määritysten pohjalta. Toteutustyön laatuun kannattaa kiinnittää huomiota. Sovelluksen dokumentaatio ja käyttöohjeet syntyvät luontevimmin toteutustyön yhteydessä.

Olennaisen osana toteutusvaiheeseen kuuluu työn tulosten testaus. Kunkin modulin alkutestaus on ohjelman tekijän tehtävä, mutta myös tekijästä riippumaton testaus on tarpeen. Tekijästä riippumaton testaus auttaa löytämään toteutuksen puutteet ja virheet, sillä tekijä itse on usein sokea omille virheilleen. Testiaineiston on oltava riittävän monipuolinen ja laaja. Kriittisissä sovelluksissa jo toteutusvaiheeseen on syytä sisällyttää lähdekoodin tarkastus.

Testauksen tulokset dokumentoidaan. Hyväksytyn testauksen jälkeen voidaan aloittaa järjestelmän käyttöönotto.

Turvatoimien toteutuksen tehtävät

TURVATOIMIEN TOTEUTUS

- ***Toteutetaan suunnitellut turvatoimet***
- ***Testataan turvatoimet ja kontrollit***
- ***Sisällytetään turvatoimet varsinaisiin toimintoihin***

Aiemmissa vaiheissa on tehty määritykset turvatoimien toteutukseen. Tätä toteutusta ohjaavat myös lait, standardit ja yrityksen omat turvallisuutta koskevat periaatteet ja ohjeet. Turvatoimien toteutus sisältyy mm. tehtäviin ohjelmiin, käyttöohjeisiin sekä järjestelmän käyttövaltuuksien ja käyttäjäprofiilien määrityksiin.

Järjestelmän turvallisuus toteutetaan edellä kuvattujen toteutusta ohjaavien tekijöiden mukaan. Turvatoimet, kuten muukin osa järjestelmää, on testattava. Paitsi ohjelmat, myös käyttöympäristö, ohjeet ja toimintatavat vaativat testaamista. Tulevan, tuotannon aikaisen ylläpitoympäristön turvatoimien testaus on myös toteutusvaiheessa huomioonotettava asia.

Kehittämisen aikana on huolehdittava työn tulosten turvaamisesta asianmukaisin varmistusmenettelyin sekä huolehdittava kehitysympäristön turvatoimista. Käyttövaltuudet myös kehitysympäristöön pitäisi antaa työtehtävien edellyttämässä laajuudessa. Toteutuksen valmistuttua kehitysympäristön käyttövaltuudet poistetaan.

Turvatoimien toteutukseen vaikuttaa suuresti järjestelmän tekninen ympäristö. Tähän kuuluvat mm. laitteisto, käyttöjärjestelmä, tietokanta-ohjelmisto ja käytettävä sovelluskehitin.

Turvatehtävien päätulokset

Toteutusvaiheen tuloksena syntyy testattu järjestelmä, johon kuuluvat kiinteästi myös turvatoimet toteuttavat ohjelmamoduulit. Turvatoimien toteutus on myös dokumentoitava. Ilman hyvää dokumentaatiota järjestelmän käytön aikaisten ongelmien selvittely ja ylläpito on erittäin hankala tehtävä. Yksittäisten ohjelmamoduulien dokumentaatio sisältyy ohjelmien lähdekoodiin, mutta yleisemmän tason kuvauksiakin tarvitaan.

- ***Turvatoimien testatut ohjelmamoduulit***
- ***Testattu tietojärjestelmä***
- ***Turvatoimien testauspöytäkirjat***
- ***Turvatoimien käyttöohjeet***

Turvatoimista tulee laatia myös käyttöohjeet. Näitä käyttöohjeita on eri tasoisia riippuen käyttäjäryhmästä (sovellusten peruskäyttäjät, pääkäyttäjät, ylläpitohenkilöstö, tietokannanhoitaja, ...).

Turvatoimien testauksen tuloksena syntyvät testauspöytäkirjat. Näistä tulee käydä ilmi mm. testaajat, käytetty testiaineisto ja testien tulokset.

Jo toteutusvaiheessa joudutaan ottamaan kantaa siihen, millaisessa ympäristössä tuotannon aikaista testausta suoritetaan. Testaus on tarpeen mm. tuotannon aikaisten ongelmien selvittelyssä ja ohjelmamuutosten toimivuuden toteamisessa. Tuotannon aikaisesta testausympäristöstä tulee laatia oma turvakuvaus.

Järjestelmän käyttöönotto

Helvi Salminen,
Tietoturva-asiantuntija,
Setec Oy

Käyttöönottovaihe on yksi järjestelmän elinkaaren kriittisistä vaiheista. Käyttöönottovaiheen testauksissa pyritään todentamaan järjestelmän toimivuus. Vaihe on tärkeä tarkastuspiste ja viimeinen tilaisuus sada kiinni järjestelmässä mahdollisesti piilevät kriittiset virheet ennen järjestelmän siirtoa tuotantoon.

Vaiheen tarkoitus ja toiminnot

Systeemi- ja käyttöönottotestauksien hyväksymisen jälkeen toiminta siirretään käyttäjien ja tukiorgani-saatioiden vastuulle. Turvatoimien käyttöönotto on osa käyttöönottoprosessia.

Käyttöönottovaiheessa testataan koko järjestelmä kaikkine laitteineen ja ohjelmistoineen. Käyttöönottotestausta varten tulee laatia testaussuunnitelma, joka kattaa sekä normaalitoiminnan että poikkeustilanteet. Turvatoimien käyttöönotto on osa koko järjestelmän käyttöönottoa. Erityistä huomiota turvatoimien testauksessa on kiinnitettävä poikkeustilanteiden käsittelyyn ja toteutettujen kontrollien toimivuuteen.

Ennen tai osana käyttöönottovaihetta käyttäjille annetaan riittävä koulutus ja he osallistuvat käyttöönottotestaukseen. Käyttäjille testaus on myös osa uuden järjestelmän tuotantokäyttöön harjaantumista, joten heidän huomionsa kiinnittyy yleensä järjestelmän normaalitoimintoihin, vähemmän poikkeustilanteisiin. Täten käyttäjien tekemä testaus ei yksinään riitä käyttöönottotestaukseksi.

Käyttäjä-testaajien lisäksi tarvitaankin yleensä asiantuntija-testaajaa, joka käy läpi systemaattisesti mm. poikkeustilanteiden hallinnan, erilaiset toimintoketjut, turvatoimet ja kontrollit. Asiantuntija-testaajalta edellytetään peruskäyttäjää laejempaa ja syvällisempää tietotekniikan osaamista sekä erilaisten testauksessa käytettävien työkalujen hallintaa.

Turvatoimien käyttöönoton tehtävät

TURVATOIMIEN KÄYTTÖÖNOTTO

- ***Suoritetaan turvatoimien käyttöönottotestaus***
- ***Suoritetaan testaus integroidussa ympäristössä***
- ***Suoritetaan hyväksyntätestaus***
- ***Tarkennetaan turvakuvauksia***

Turvatoimien käyttöönotto valmistellaan nimeämällä niille vastuuhenkilöt, joille annetaan riittävät käyttövaltuudet. Käyttäjille ja tukiorganisaatiolle annetaan turvatoimia koskeva koulutus.

Testaussuunnitelman mukaisesti edeten testataan järjestelmän turvatoimet. Testauksen tulee kattaa sekä tekninen toteutus että hallinnolliset menettelyt ja ohjeet. Testaustulokset hyväksytetään henkilöllä, jolla on hyväksyntään tarvittavat valtuudet.

Jos käyttöönottotestauksessa havaitaan käyttöönoton estäviä toiminnallisia puutteita tai virheitä, järjestelmä palautuu johonkin edeltävistä vaiheista. Hyväksytty järjestelmä turvatoimineen siirretään tuotantoon käyttäjien ja tukiorganisaatioiden vastuulle.

Käyttöönottovaiheessa viimeistellään järjestelmän turvakuvaus. Kehittämis- ja testausympäristöt puretaan niiltä osin kuin ne eivät ole tarpeen järjestelmän ylläpidossa. Testauksen aikaiset käyttövaltuudet poistetaan. Projektin aineisto arkistoidaan, tarpeettomat aineistot tuhotaan.

Käyttöönoton turvatehtävien päätulokset

TURVATEHTÄVIEN PÄÄTULOKSET

- ***Turvatoimien testauspöytäkirjat***
- ***Turvattu tietojärjestelmä***
- ***Koulutetut käyttäjät***
- ***Turvaohjeistot***
- ***Turvakuvaus***
- ***Arkistoitu aineisto***

Käyttöönottovaiheen päätuloksena on toimiva tietojärjestelmä, jonka turvallisuus täyttää asetetut vaatimukset. Turvallisuuden toimivuus on varmennettu kattavin käyttöönottotestein, joiden tuloksena syntyneet testauspöytäkirjat arkistoidaan sovitun ajan.

Turvallisuus ei ole pelkkää tekniikkaa, keskeistä on ihmisten toiminta. Hyvin hoidetun käyttöönoton jälkeen käyttäjille on myös turvatoimista riittävä koulutus ja ohjeet.

Turvakuvaukseen on dokumentoitu keskeiset kehitetyn järjestelmän turvallisuuteen liittyvät asiat, ei kuitenkaan turvatoimien toteutuksen yksityiskohtia. Kuvaus itsessään on usein turvallisuusluokiteltua aineistoa, jota vastuuhenkilöt käyttävät apuvälineenä mm. järjestelmän edelleen kehittämisessä ja sen toimintojen tarkastamisessa.

Tuotantojärjestelmän käyttövaltuudet annetaan työtehtävien ja vastuun edellyttämässä laajuudessa. Erityistä tarkkuutta vaativat kehitys- ja huoltohenkilöiden oikeudet. Kriittisissä järjestelmissä tuotantoympäristön turvallisuus on vielä erikseen tarkistettava.

Järjestelmän ylläpito

Helvi Salminen,
Tietoturva-asiantuntija,
Setec Oy

Käyttöönoton jälkeen järjestelmään joudutaan usein tekemään pieniä muutoksia. Muutosten yhteydessä on tarkasteltava myös niiden vaikutuksia turvatoimiin, joihin on tehtävä muuttuneen tilanteen vaatimat muutokset.

Vaiheen tarkoitus ja toiminnot

Ylläpitovaiheen aikana korjataan järjestelmässä havaittuja virheitä ja toiminnallisia puutteita. Järjestelmään saatetaan myös lisätä alunperin toteuttamatta jääneitä ominaisuuksia. Järjestelmässä tuotantokäytön aikana havaittujen virheiden korjaus on osa ylläpitoa.

Ylläpitotoimissa toistuvat pienessä mittakaavassa järjestelmäkehityksen vaiheet.

Yrityksen tietoturvapolitiikassa ja ohjeissa tulisi olla määritelty ohjelmamuutosten käyttöönottomenettely ja siihen liittyvät vastuut. Menettelyjä tulee noudattaa myös silloin, kun järjestelmässä havaitaan käyttöönoton jälkeen vakava virhe, joka vaatii välitöntä korjaamista. Tehtävän muutoksen vaikutukset järjestelmän muihin osiin analysoidaan ja muutokset testataan kehitysympäristössä ennen käyt-töönottoa.

Turvatoimien ylläpito

Tehtäessä järjestelmään muutoksia tarkistetaan, aiheuttaako toiminnallinen muutos muutoksia myös turvatoimiin. Turvatoimien muutostarve voi syntyä myös siitä, että tuotantokäytössä olevan järjestelmän turvatoimet havaitaan riittämättömiksi tai liian tiukoiksi. Muutoksista tehdään suunnitelma, joka hyväksytetään. Toteutus tehdään hyväksytyn suunnitelman pohjalta.

- ***Suunnitellaan ja toteutetaan järjestelmän muutosten turvatoimiin aiheuttamat muutokset***
- ***Testataan ja otetaan käyttöön turvatoimien muutokset. Käyttäjille koulutus muutoksista.***

Turvatoimien muutokset on testattava huolellisesti testausympäristössä ennen niiden käyttöönottoa. Muutokset voidaan siirtää tuotantoon, kun ne on asianmukaisesti testattu ja hyväksytetty.

Turvatoimien muutokset ovat joskus luonteeltaan teknisiä, eivätkä näy suoraan järjestelmän käyttäjille. Osa muutoksista sen sijaan vaikuttaa näkyvästi käyttäjien työskentelyyn. Näiltä osin käyttäjille annetaan muutoksia koskeva koulutus ja käyttöohjeisiin tehdään tarvittavat muutokset.

Turvatehtävien päätulokset

- ***Turvatoimien muutosten vaatimukset ja määrittelyt***
- ***Testatut turvatoimien muutokset***
- ***Turvatoimien testauspöytäkirjat***
- ***Turvatoimien käyttöohjeet***
- ***Muutoksiin koulutetut käyttäjät***

Ylläpitovaiheessa tehtävien muutosten tulee perustua todettuun muutostarpeeseen ja sen perusteella laadittuun hyväksyttyyn suunnitelmaan. Muutoksen päätuloksia ovat testatut ja hyväksytyt turvatoimien muutokset.

Kuten alunperin toteutusvaiheessa, myös ylläpitoaikaisista muutoksista laaditaan testauspöytäkirjat ja muuttuneiden toimintojen käyttöohjeet. Jos turvatoimien muutokset vaikuttavat käyttäjien päivittäiseen työskentelyyn, heille annetaan koulutus myös muuttuneiden turvatoimien osalta.

Järjestelmän version vaihto

Helvi Salminen
Tietoturva-asiantuntija,
Setec Oy

Toisinaan, esimerkiksi organisaation toimintaprosessien muuttuessa, järjestelmiin on tarvetta tehdä normaalia ylläpitoa suurempia muutoksia. Tällaisissa projekteissa muutosten hallinnassa ja tietoturvallisuudessa on joitakin erityispiirteitä, joista hieman tarkemmin seuraavassa.

Versiomuutoksen tarkoitus ja toiminnot

Tietojärjestelmän merkittävät versiomuutokset liittyvät usein muutokseen siinä toiminnassa, jota järjestelmä palvelee. Muutoksen voi käynnistää myös järjestelmän laitteiston käyminen riittämättömäksi kapasiteetiltaan kasvaneeseen toimintaan. Myös ohjelmistototeutuksessa saattaa olla piirteitä, jotka tietomäärän kasvaessa eivät enää ole toimivia.

Version vaihdossa on paljolti samoja piirteitä kuin ensikehittämisprojektissa, jonka eri vaiheita on käsitelty edellisissä artikkeleissa. Oman mutkikkuutensa tekniseen toteutukseen tuo se, että vanhan järjestelmän sisältämät tiedot on konvertoitava uuteen ympäristöön.

Tietojen siirto vanhasta järjestelmästä uuteen

Järjestelmän toiminnallisten muutosten yhteydessä muuttuvat yleensä myös sen tietorakenteet. Tällöin tiedot on muunnettava uuden järjestelmän rakenteisiin sopivaksi. Koska uusi järjestelmä toimii tehokkaammassa laitteistoympäristössä, varsinainen tietojen konversio kannattaa tehdä uudessa ympäristössä. Vanhassa järjestelmässä tiedot muunnetaan uuden järjestelmän ymmärtämään muotoon.

Siirron täydellisyys ja tietokantojen eheys siirron jälkeen tulee varmistaa mm laskemalla tietokantarivien lukumäärät ennen ja jälkeen siirron. Myös joidenkin tietokantakenttien summakontrollit sekä tiedon arvoalueen ala- ja ylärajojen tarkistukset auttavat varmistumaan siirron onnistumisen. Tietoaineistosta kannattaa myös ottaa näytteitä tarkastelemalla tarkoituksenmukaisilla kriteereillä valittujen tietueiden koko sisältöä.

Tiedon eheyden lisäksi siirrossa tulee muistaa huolehtia myös tietojen luottamuksellisuudesta. Siirrossa mahdollisesti käytettävien välitiedostojen suojaukset eivät välttämättä ole yhtä tiukkoja ja hienojakoisia kuin tietokannan suojaukset. Siirron aikana tietoihin pääsevät mahdollisesti käsiksi tekniset asiantuntijat, joilla ei normaalitilanteessa ole käyttövaltuuksia kyseisiin järjestelmiin. Siirron kontrollimenettelyissä on siis otettava huomioon myös tietojen turvallisuusluokitus ja siirtomenettelyt suunniteltava sen vaatimusten mukaisiksi.

Uuden ja vanhan järjestelmän rinnakkainen käyttö

Rinnakkaiskäyttö on mahdollista pienissä järjestelmissä, joissa manuaalisesti käsiteltävän tiedon määrä on suhteellisen vähäinen. Myös uuden ja vanhan järjestelmän tuottamien tulosten on oltava helposti vertailtavissa keskenään.

Rinnakkaiskäytön huono puoli on sen resursseja kuluttava vaikutus. Hyvänä puolena on se, että järjestelmä testataan todellisessa käyttötilanteessa, jolloin siinä tuotantokäytön alkaessa todennäköisesti on suhteellisen vähän toiminnallisia ongelmia ja käyttäjät ovat harjaantuneita järjestelmän käyttöön. Rinnakkaiskäyttö ei poista asiantuntijatestauksen tarvetta, jossa järjestelmään toimintoja tutkintaan “pintaa syvemmältä“.

Järjestelmien versiointi

Laajoissa, monimutkaisissa järjestelmissä rinnakkaiskäyttö ei ole mahdollista. Tällöin uuden version toiminta on testattava mahdollisimman kattavasti erillisessä kehitysympäristössä. Käyttöönotto on, riippuen järjestelmän rakenteesta ja toimintaympäristöstä, mahdollista tehdä paloittain tai yhdellä kertaa.

Väistyvän järjestelmäversion tietoja ja ohjelmia voidaan eri syistä joutua säilyttämään pitkiäkin aikoja (ks. artikkeli **Järjestelmän poisto käytöstä**). Käytettäessä järjestelmäkehityksessä versionhallintatyökaluja eri versiot arkistoidaan hallitusti. Ongelmien ilmetessä on mahdollista palauttaa tuotantoon vanha versio, jos muutokset ovat teknisiä eivätkä johdu peruuttamattomista muutoksista ympäristössä (esim. Y2K) tai toiminnoissa, joihin järjestelmä liittyy.

Mitä tehdään vanhalle järjestelmälle

Vanhan järjestelmän käyttöohjeet ja dokumentaatio kerätään pois käyttäjiltä. Vanhentuneet ohjeet saattavat aiheuttaa käyttäjien keskuudessa tarpeetonta hämmennystä ja suuren määrän tahattomia virheitä.

Laitteiden käytöstä poistoa ja tallenteiden hävittämistä käsitellään tarkemmin järjestelmien käytöstä poistamista koskevassa artikkelissa.

Muutosprosessi käyttäjien näkökulmasta

Käyttäjien tulee saada riittävä koulutus, jotta muutos vanhasta uuteen sujuisi mahdollisimman kitkattomasti. Muutosvastarintaan on syytä kiinnittää huomiota. Muutoin käyttäjät helposti haikailevat takaisin “vanhoja hyviä aikoja“, jolloin välttämättömät toiminta- ja ajattelutapojen muutokset viivästyvät.

Järjestelmän poisto käytöstä

Helvi Salminen,
Tietoturva-asiantuntija,
Setec Oy

Järjestelmän elinkaaren viimeinen vaihe on sen poisto käytöstä. Tähänkin vaiheeseen sisältyy tietoturvallisuuden kannalta merkittäviä tehtäviä, mm. aineiston hävittämistä ja käyttövaltuuksien hallintatoimenpiteitä.

Vaiheen tarkoitus ja toiminnot

Järjestelmän käytöstä poisto on sen elinkaaren viimeinen vaihe. Poisto on syytä tehdä suunnitelmallisesti ja sen vaikutukset jäljelle jääviin toimintoihin on analysoitava sekä korvaavat menettelyt suunniteltava ja otettava käyttöön. Tarpeettomaksi käynyt aineisto on hävitettävä turvaluokituksen edellyttämällä tavalla.

Mitä voidaan hävittää

Kaikkea käytöstä poistettavaan järjestelmään liittyvää aineistoa (ohjelmat, tiedot, dokumentti ...) ei voida hävittää käytöstä poiston yhteydessä. Lainsäädäntö (esimerkiksi kirjanpitolaki) tai yrityksen tekemät sopimukset voivat edellyttää aineiston, mukaanlukien ohjelmat, säilyttämistä määrätyn ajan.

Tällöin käytöstä poiston sijasta on oikeampaa puhua järjestelmän passivoinnista. Varsinainen poisto voidaan tehdä vasta kun lakien tai sopimusten edellyttämä säilytysaika on kulunut umpeen.

Esimerkkejä aineiston hävittämiseen liittyvistä tietoturvaongelmista

Useimmille lienevät tuttuja aika ajoin julkisuuteen putkahtaneet tiedot epäasiallisista menettelyistä arkaluontoisen aineiston käsittelyssä. Esimerkiksi tietojen poisto on laiminlyöty joissakin tapauksissa, joissa salassapidettävän aineiston käsittelyssä käytettyjä laitteita on myyty edelleen muuhun käyttöön, minkä seurauksena arkaluontoista tietoa on paljastanut asiattomille.

Tietoaineiston hävittämisestä

Järjestelmän käytön aikana syntyy aineistoa, joka pitää asianmukaisesti hävittää. Tällaista aineistoa ovat mm. järjestelmän tuottamat tulosteet, kierrosta poistettavat varmistusmediat ja aineiston käsittelyssä käytettävien laitteiden rikkoontuneet kiintolevyt. Kun järjestelmän käyttö lopetetaan kokonaan, hävitettävän aineiston määrä voi olla hyvinkin suuri.

Tietoaineistolle sopivat hävittämismenettelyt riippuvat aineiston turvaluokituksesta. Aineiston hävittämisestä on laadittu ohjeita, joista pieni ote seuraavassa:

- **Julkinen** tai **sisäiseen käyttöön** tarkoitettu vanhentunut aineisto hävitetään. Julkisen aineiston hävitystapa on vapaa, sisäisen aineiston hävityksen on oltava kunnolla organisoitu.
- **Luottamuksellinen** aineisto hävitetään valvotusti. Paperi- tms. aineisto silputaan tai poltetaan. Tallenteet päällekirjoitetaan tai demagnetoidaan, jos mediat halutaan uudelleen käyttöön. Kokonaan käytöstä poistettavat mediat tuhotaan fyysisesti.
- **Salaisen** aineiston hävittäminen tapahtuu tiedon omistajan luvalla, hävittämisestä vastaavat nimetyt henkilöt. Hävitystoimenpiteistä pidetään kirjaa. Paperiaineisto poltetaan tai silputaan, järjestelmien tallenteet tuhotaan fyysisesti.
- **Erittäin salainen** hävitettävä aineisto palautetaan omistajalle, joka arkistoi siitä tarvittavat osat. Tämän luokan aineisto hävitetään erikseen, ei muun aineiston yhteydessä. Aineiston omistaja vastaa hävitystoimenpiteistä ja niihin liittyvästä kirjanpidosta. Hävitysmenettelyt kuten salaisella aineistolla.

Miten välttyä ongelmilta ?

Keinoja välttää ongelmia ovat mm. seuraavat:

- Kaikki poistettavaa järjestelmää koskevat ohjeet ja dokumentaatio kerätään pois käyttäjiltä. Näin vältytään virheellisten toimintaohjeiden aiheuttamalta sekaannukselta.
- Käyttövaltuuksien hallintamenettelyillä taataan, että kaikki järjestelmän käyttöön liittyvät oikeudet organisaation verkkoon ja tietokantoihin poistetaan. Jäljelle jäävien järjestelmien käyttö ei saa häiriintyä toimenpiteiden seurauksena. Käyttövaltuuksien muutokset hoituvat helpommin, jos hallinta on toteutettu hyvin suunnitelluilla käyttäjäprofiileilla.
- Käytöstäpoistopäätöksen yhteydessä analysoidaan poistettavan järjestelmän liittymät muihin järjestelmiin. Poistettavan järjestelmän osuus korvataan tarvittaessa uusilla toiminnoilla tai liittymät “ajetaan alas“ hallitusti.
- Tietojen hävittämisestä huolehditaan edellä kuvatulla tavalla.

Kenen vastuulla ovat hallitun käytöstä poistamisen turvatoimet

Organisaation toimintaohjeissa tulisi olla määritelty vastuut järjestelmien käytöstä poistamisen turvatoimista. Järjestelmän kehittäjille kuuluu luontevimmin käytöstä poiston muihin järjestelmiin ulottuvien vaikutusten analysointi sekä tarvittavien järjestelmämuutosten suunnittelu ja toteuttaminen.

Sähköinen tunnistus

Aarno Kansikas,
Johdon konsultti,
ICL Konsultointi

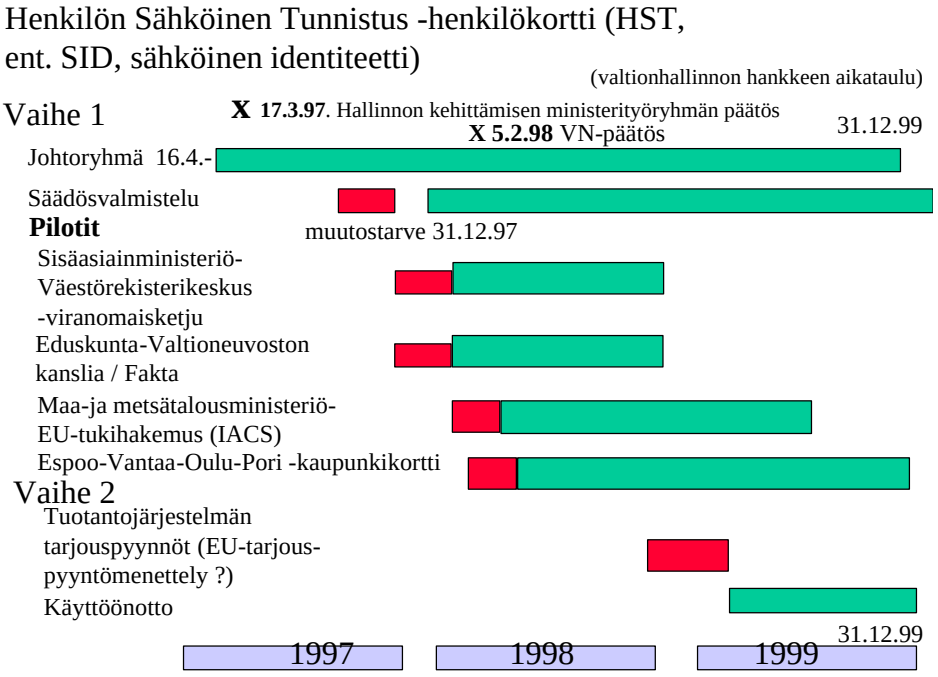
Tietoturvallisuusluokitukset järjestelmäkehityksessä johtavat mm. henkilöiden vahvan tunnistuksen ja käyttöoikeuksien todentamisen tarpeeseen. Tähän on parhaillaan kehitteillä valtakunnallinen infrastruktuuri.

Kansallinen sähköisen tunnistuksen infrastruktuuri

Hallinnossa on käynnissä useita sähköisen asioinnin kehittämishankkeita. Valtiovarainministeriö julkisti 27.9.1996 ehdotuksen kansalliseksi sähköisen tunnistuksen tietoturvallisuusinfrastruktuuriksi Raportin valmistelussa ovat olleet mukana myös liikenneministeriö ja sisäasiainministeriö. Hallinnon kehittämisen ministerityöryhmä on 7.3.1997 päättänyt, että Suomeen toteutetaan yksi yhteinen sähköinen tunnistamistapa.

Hankkeen toteuttamisen johtoryhmä on asetettu 16.4.1997. Valtioneuvosto teki asiasta periaatepäätöksen 5.2.1998. Säädösmuutosvalmisteluhanke on vireillä. Hankkeen määräaika on vuoden 1999 loppu.

Henkilön sähköinen tunnistaminen toteutetaan toimikorttiteknologiaan ja julkisen avaimen menetelmään perustuvana ratkaisuna, joka otetaan käyttöön asteittain vuodesta 1999 alkaen. Hankkeen ajoituspuitteet on esitetty kuvassa 1.



Kuva 1

Piloteissa testataan sisäasiainministeriön / väestörekisterikeskuksen viranomaisketjun toimintaa varmennustehtävissä, SGML-muotoisen sähköisen asiakirjan kulkua järjestelmässä eduskunnan ja valtioneuvoston välillä, maanviljelijöiden EU-tukihakemuksen tekoa Internetin välityksellä suoraan Maa- ja metsätalousministeriön järjestelmään sekä kaupunkikorttia Espoossa, Vantaalla, Oulussa ja Porissa. Viimemainittuun sisältyy tunnistusominaisuuksien lisäksi noin kymmenen muuta toimintoa mm. maksukorttiominaisuus.

Henkilökortti

Henkilökortti (Finnish Electronic Citizen Card, kuva 2) sisältää vain välttämättömät luotettavaan tunnistamiseen tarvittavat tiedot. Ratkaisut toteutetaan siten, että niitä voidaan hyödyntää myös sähköisessä kaupankäynnissä ja muissa yksityissektorin tehtävissä.

Henkilökortin hankkiminen olisi vapaaehtoista ja sitä voitaisiin sähköisen tunnistamisen lisäksi käyttää henkilön kuvalla varustettuna myös näytettävänä henkilöllisyystodistuksena.

Kuva 2

Valtioneuvoston periaatepäätös sähköisestä asioinnista

Valtioneuvosto on päättänyt (Valtioneuvoston periaatepäätös sähköisestä asioinnista, palveluiden kehittämisestä ja tiedonkeruun vähentämisestä, 5.2.1998, VM 9/00/98), että ryhdytään valmistelemaan ja toteuttamaan seuraavia toimenpiteitä edellyttäen, että Eduskunta ne osaltaan hyväksyy.

1. HALLINNON SÄHKÖINEN ASIOINTI

   1.1 Nimetään Väestörekisterikeskus valtion sähköisen henkilökortin antamisesta ja ylläpidosta vastaavaksi varmenneviranomaiseksi ja luodaan muu tarvittava varmenneviranomaisorganisaatio ja palvelut.

   1.2 Toteutetaan ja otetaan käyttöön vuonna 1999 kaikille kansalaisille tarkoitettu maksullinen henkilökortti, joka toimii henkilön sähköisen tunnistamisen ja allekirjoituksen välineenä.

   1.3 Oikeusministeriö ja muut ministeriöt valmistelevat hallinnon sähköisen asioinnin, sähköisen asiakirjan ja allekirjoituksen sekä henkilökortin ja varmenneviranomaispalveluiden edellyttämän lainsäädännön 30.6.1999 mennessä.

   1.4 Toteutetaan vuoden 1998 loppuun mennessä EU-maiden väliseen yhteistyöhön ja kotimaisiin tarkoituksiin tarvittava julkisen hallinnon hakemistopalvelu, joka sisältää sähköpostiosoitteet ja muut tarvittavat yhteystiedot.

2. PALVELUIDEN KÄYTÖN TEHOSTAMINEN

   2.1. Ministeriöt ja virastot huolehtivat siitä, että tiedot keskeisistä kansalaisille, yrityksille ja yhteisöille suunnatuista palveluista ja niissä tarvittavista lomakkeista ovat saatavina molemmilla kotimaisilla kielillä verkoissa ja merkittävä osa hakemuksista ja anomuksista voidaan myös saattaa verkkojen kautta vireille vuoteen 2001 mennessä.

   2.2. Viranomaiset kehittävät hallinnon tarvitsemia sähköisiä asiakirjoja ja asiointipalveluita sekä yhteispalvelujen tarjontaa tämän päätöksen mukaisesti.

3. TIEDONKERUU

   3.1 Valtion viranomaiset vähentävät ja rationalisoivat tiedonkeruuta tavoitteena tiedonkeruun kustannusten vähentäminen vähintään kolmanneksella vuodesta 1997 vuoteen 2002.

   3.2 Viranomaisten tiedonkeruun lainsäädännölliset yleisvaltuudet poistetaan ja erityisvaltuudet rajataan lakisääteisesti niihin tietoryhmiin, jotka ovat välttämättömiä viranomaistehtävien hoitamiseksi. Samalla kehitetään rekistereiden yhteiskäyttöä ja tietopalveluja.

   3.3 Valtiovarainministeriön ja sisäasiainministeriön tulee yhteistyössä Tilastokeskuksen kanssa ohjata tiedonkeruun vähentämiseen liittyvien toimenpiteiden toteutumista.

   3.4. Hallinnon kehittämisen ministerityöryhmä selvittää EU:n toimielinten kanssa toimenpiteitä, joilla EU:n keräämien tietojen määrää sekä keräämisestä ja toimittamisesta aiheutuvaa työtä ja kustannuksia voidaan nykyisestään vähentää.

4. TOIMEENPANO JA SEURANTA

   Valtiovarainministeriö ja sisäasiainministeriö vastaavat tämän päätöksen toimeenpanosta ja seurannasta ja raportoivat tästä valtioneuvostolle vuosittain vuodenvaihteessa sekä antavat yhdessä muiden viranomaisten kanssa tähän liittyviä ohjeita ja suosituksia.

Mihin perustuu tunnistuksen turvallisuus?

Sähköinen tunnistus ja Henkilökortti ovat tietoteknisiä välineitä, joiden avulla tietoturvallisuutta ja tietosuojaa voidaan tehostaa merkittävästi.

Varmennusorganisaatio ei luovuta muuhun käyttöön sähköisen identiteetin käyttötietoja. Salaiset avaimet hävitetään kortille alustuksen yhteydessä, ne jäävät vain kortille. Key escrow -periaatetta (eli viranomaisen salauksen avausmahdollisuutta, yleisavainjärjestelmää) ei sovelleta Suomessa. Ns. vapaaehtoinen key recovery -toiminne on suunnitteilla. Kortti on

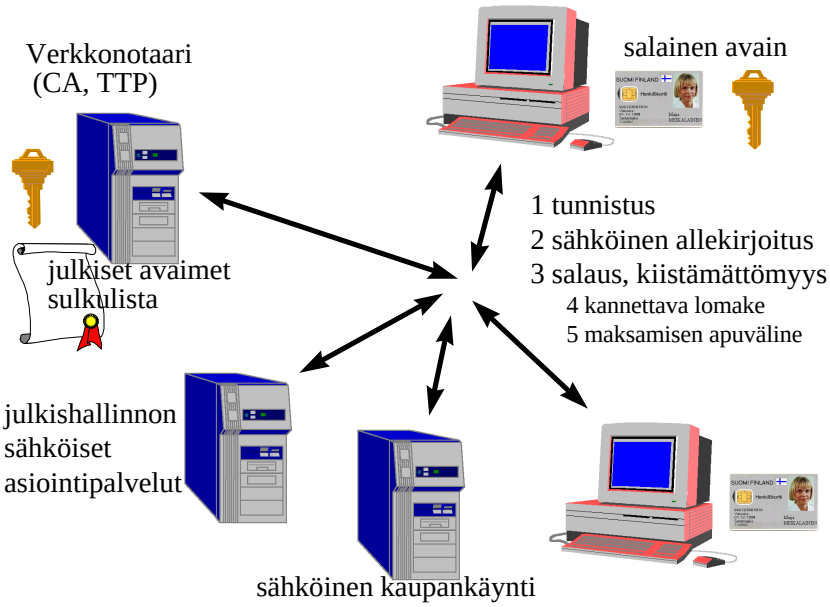
määräaikainen ja infrastruktuurissa käytettävät krypto- yms. teknologiat uusitaan tarpeen vaatiessa.

Kortin tietoja ei voi kopioida tai muuttaa ilman kortin antajan hallintakorttia ja kortinlukijaan liittyvää varmistusohjelmistoa, turvamodulia.

Järjestelmä voidaan liittää vastaaviin muihin korttijärjestelmiin ja kansainvälisiin varmennusjärjestelmiin ylimmän varmennusviranomaisen (CA) kautta. Pohjoismaat, etenkin Ruotsi ja Tanska suunnittelevat yhdessä järjestelmää, Singapore on ottanut vastaavan järjestelmän koekäyttöön kesällä 1997, Kanada ja Australia tähtäävät seuraaviksi Suomen jälkeen ja muita uusia suunnitelmia on vireillä.

Sähköinen tunnistaminen perustuu ns. Julkisen avaimen infrastruktuuriin (PKI, kuva 3), henkilökortilla oleviin henkilötietoihin ja salaisiin avaimiin sekä julkisiin avaimiin, jotka sijaitsevat varmennehakemistoissa luotetuilla kolmansilla osapuolilla.

Avainparin avulla luotua asiakirjaa voidaan tulkita vain julkisen avaimen avulla, jolloin varmistutaan asiakirjan tekijästä. Toisaalta taas julkisella avaimella salatun tekstin voi tulkita ainoastaan salaisen avaimen haltija. Järjestelmä mahdollistaa useamman avainparin käytön, esim. eri avainparit allekirjoitukseen, todentamiseen ja salaukseen.



Kuva 3

Ns. Luotetun kolmannen osapuolen (verkkonotaari, TTP) palveluihin kuuluvat myös sulkulista kadonneita tai muuten käyttökiellossa olevia kortteja varten ja aikaleimapalvelut kiistämättömyyden osoittamiseksi.

Siihen liittyvän tekniikan ja luotettujen kolmansien osapuolien avulla voidaan toteuttaa riittävän turvallisesti mm. osapuolten tunnistus ja todennus, sähköinen allekirjoitus, siirrettävän asiakirjan salaus ja asioinnin kiistämättömyys. Lisäksi teknologia mahdollistaa Henkilökortin käyttämisen kannettavana sähköisenä asiakirjana ja maksamisen mahdollistavana välineenä.

Anonyymi asiointi on edelleen mahdollista niissä tilanteissa, jotka eivät nykyisinkään manuaaliasioinnissa edellytä tunnistamista tai rekisteröintiä. Kortille tulevat muut mahdolliset sovellukset ratkaistaan myöhemmin eri hankkeissa ao. viranomaisten ja tietosuojaviranomaisten kesken. Samoin myöhemmin ratkaistaan useamman kortin tarve mm. voivatko muut vastaavat kortit toimia Henkilökorttina sähköisen tunnistamisen varmistajana ja päinvastoin. Anonyymipalveluita luotetun kolmannen osapuolen toimesta tullaan kehittämään.

Varmennepalveluita ja ns. Luotetun kolmannen osapuolen eli verkkonotaarin palveluita tullaan tuottamaan useiden osapuolten toimesta. Valtionhallinnon ylimmäksi varmenneviranomaiseksi on nimetty Väestörekisterikeskus.

Varmennusorganisaation järjestelmien turvallisuus

Kortin valmistuksen ja kuljetuksen osalta edellytetään että kortin valmistusprosessin turvallisuustason tulee vastata korkeita turvavaatimuksia. Kortit on loogisesti suojattava kuljetuksen ajaksi (kortin alustajalle)

Kortin alustamisessa tehdään seuraavat toimenpiteet: kortin sarjanumeron kirjoittaminen kortille (ellei ole tapahtunut valmistajan toimesta), salaisten avainten tallentaminen kortille, HST-sovelluksen alustaminen kortille

Kortin yksilöinti ja jakelu / luovutus haltijalle:

- kortinhaltijan henkilöllisyys on varmistettava sekä haku- että luovutusvaiheessa
- kortinhaltijalta on vaadittava kuittaus kortin vastaanottamisesta ja kortin käyttöä koskevien ehtojen kirjallinen hyväksyntä
- kortinhaltijoita koskevia tietoja on käsiteltävä riittävän turvallisin menettelyin niiden eheyden ja luottamuksellisuuden varmistamiseksi.

Korttikannasta on ylläpidettävä rekisteriä, joka sisältää ainakin seuraavat korttikohtaiset tiedot

- kortin sarjanumero
- kortin luovutuspäivä kortinhaltijalle
- kortinhaltijan nimi ja henkilötunnus
- kortin visuaaliset tiedot
- kortin viimeinen voimassaolopäivä

Korteista on ylläpidettävä sulkulistaa siihen liittyvine tietoineen (eri asia kuin varmenteita koskeva sulkulista)

Avaingeneroinnin järjestelmien turvallisuus

HST-järjestelmässä eri osapuolten käyttämät julkisen avaimen menetelmän avainparit eroavat toisistaan käyttötarkoituksen ja omistajansa aseman suhteen. Tämän johdosta avaimet on luokiteltava seuraavasti:

- varmentajan (VA) avaimet
- rekisteröijien (RE) avaimet
- HST-järjestelmän hallintakäyttäjien avaimet
- kortinhaltijoiden avaimet

Kunkin ryhmän avaimet luokitellaan ko. avainten käyttötarkoituksen mukaan. Käyttötarkoitukset voivat olla eri ryhmillä erilaiset (esimerkiksi varmentajalla saattaa olla erityinen avain vain sulkulistan allekirjoittamista varten). Avainten luokitusta käytetään erilaisten käsittelysääntöjen soveltamiseksi eri avainluokkiin.

Avainparin avaimista toinen valitaan jukiseksi avaimeksi ja toinen salaiseksi. Salainen avain tallennetaan sähköiselle henkilökortille välittömästi generoinnin jälkeen ja hävitetään kortin ulkopuolelta lopullisesti. Julkinen avain ja siihen kytketty kyseisen henkilökortin sarjanumero luovutetaan rekisteröijälle jatkoprosessointia varten.

Avainparin generointiprosessi on kriittinen, koska järjestelmän luotettavuuden kannalta salaisen avaimen salassapysyminen on keskeistä.

Avainten generointiin käytettävä laitteisto, sen käyttöjärjestelmä ja ohjelmistot ja täytyy olla dokumentoitu sekä varmentajan tarkastamat ja hyväksymät. Laitteisto ei saa olla yhteydessä ulkomaailmaan lukuunottamatta generointiprosessin tulosten luovuttamista. Kaikkien laitteistoon tulevien johtojen tulee olla näkyvissä. Generoitujen salaisten avainten tulee pyyhkiytyä laitteiston muistista välittömästi prosessin päättyessä. Salaisia avaimia ei saa kirjoittaa kovalevylle tai muulle massamuistilaitteelle, vaan ainoastaan haihtuvaan muistiin.

Generointiprosessin yhteydessä tai sen jälkeen tulee tarkistaa, että generoitu julkinen avain on ainutkertainen eli että sama avain ei ole jo käytössä järjestelmässä

Tilaan, jossa avainten generointiprosessi suoritetaan, saa olla pääsyoikeus ainoastaan prosessia suorittavalla tai valvovalla henkilökunnalla.

Avainten generointiprosessia suorittava tai valvova henkilökunta täytyy olla tehtävään erikseen koulutettu ja heidän soveltuvuutensa tehtäviin arvioitu.

Generointiprosessin käynnistämiseen ja suorittamiseen on vaadittava vähintään kahden järjestelmän käyttöön valitun henkilön läsnäolo.

Lähteet, kirjallisuutta

Henkilön sähköinen identiteetti ja henkilökortti, raportti 16.9.1996, Valtiovarainministeriö, Liikenneministeriö, Sisäasiainministeriö: http://www.vn.fi/vm/suomi/muuta/vahti/sidrap.htm

HST-järjestelmän tekninen määrittely: yhteiset vaatimukset pilotprojekteille 1997-11-24 http://www.vn.fi/vm/suomi/muuta/vahti/hst_ma1.htm

Valtiohallinnon tietoturvallisuuskäsitteistö, Valtionhallinnon tietoturvallisuuden johtoryhmä 18.4.1997, http://www.vn.fi/vm/suomi/muuta/vahti/sanasto.htm

Kirjoittaja

Aarno Kansikas toimii johdon konsulttina ICL Konsultoinnissa tärkeimpänä erityisosaamisalueenaan tietoturvallisuuden kehittämisprosessi. Hän on myös Tietoturva ry:n hallituksen jäsen.

puh. 09-567 3450
aarno.kansikas@icl.fi

Tietojärjestelmien tietoturvavastuut

Tuija Kyrölä,
Tietoturvakonsultti,
TietoTurvaKoulutus Oy

Tiedon turvallisuus sitä käsittelevän vastuulla

Kun organisaatiossa määritellään tiedon omistajan vastuita, ollaan oikeilla jäljillä ja yhden tietoturvallisuuden peruskysymyksen ääressä. Useimmassa yrityksessä kysymys on ohitettu tai siihen on ainoastaan viitattu jonkun kaapissa olevassa tietoturvallisuuspolitiikassa. Tiedon omistajan vastuita voidaan lähestyä kysymyksillä:
1.Miten käyttövaltuuksien hallinta järjestetään?
2.Miten toiminnan virhe- ja poikkeamatilanteet hallitaan?
3.Miten sovelluksen käyttö ohjeistetaan?
4. Miten sovellusmuutokset hyväksytetään?

Vastauksissa havaitaan, että tiedon turvaamisesta, sen eheydestä, saatavuudesta ja luottamuksellisuudesta, vastaa tiedon käsittelyketjun eri osapuolet. Käsittelyketju saattaa olla muuttunut tietohallinnon ulkoistamisen yhteydessä, jolloin kontrolleja usein jää pois käytöstä. Tietojärjestelmiin liittyvät tietoturvavastuut voidaan luokitella seuraavasti

- tietojärjestelmän käyttäminen
- tietojärjestelmän kehittäminen
- tietokonekeskus/tietojärjestelmän tuotanto
- kehityshankkeista ja ulkoisista palveluista päättävät.

Tietojärjestelmän käyttäminen

Tietojärjestelmää tai sen osaa, tiettyä sovellusta tai ohjelmaa käyttää joukko käyttäjiä. Kyseisen ohjelman tilanneen tai hankkineen yksikön vetäjä on tiedon omistaja. Tiedon omistaja on nimetty henkilö. Tiedon omistajan vastuulla on

- että tietoja käsitellään yrityksen tietoturvallisuuspolitiikan ja -ohjeiden mukaisesti
- käsitellä ja hyväksyä jokaisen käyttäjän tiedonkäsittelytarpeet ja ilmoittaa tarve kirjallisesti käyttövaltuuksia ylläpitäville
- että ohjelmaa käyttävien henkilöiden käyttövaltuudet ovat työtehtävän mukaiset
- että jokainen toimii omalla henkilökohtaisella käyttäjätunnuksellaan
- tarkastaa säännöllisesti raportti, jossa on eri henkilöiden käyttövaltuudet
- tarkastaa ja hyväksyä määrävälein tärkeiden/kriittisten tietojen ylläpidoista rekisteröitynyt tieto
- että yksikön toiminnan virhe- ja poikkeamatilanteet hallitaan
- että yksikössä on luotettavat käyttöohjeet
- että toiminnan edellyttämät varajärjestelyt suunnitelmineen ovat ajantasaiset ja henkilöstön tiedossa
- kehitteillä olevan ohjelman ja sen käsittelemien tietojen luokittelu (salainen, luottamuksellinen, sisäinen , julkinen) ja luokittelun mukaisten kontrollien vaatiminen (teksti ‘luottamuksellinen ‘ näytöillä/tulosteilla, rajatut kyselyt ja niiden lokaus,
- tarkistussummat, tietokannan salaus, tiedon siirto)
- kehitteillä olevan ohjelman testaaminen ja sen hyväksyminen käyttöön
- huolehtia, mikäli uuden ohjelman käyttöönotto ei onnistu, että toimintaa pystytään jatkamaan ennalta suunnitelluin manuaalisin menetelmin tai pystyttävä palaamaan vanhaan.

Tiedon omistaja vastaa yksikössä eri välineillä käsiteltävän tiedon oikeellisuudesta, ajantasaisuudesta ja luottamuksellisuudesta sekä saatavuudesta. Tiedon omistajan on oltava tiiviissä yhteistyössä uutta ohjelmaa/sovellusta määriteltäessä. Koska tiedon omistaja vastaa asiakkaille yksikön palvelun laadusta, oikeellisuudesta, ajantasaisuudesta, luotettavuudesta ja toiminnan tarkastettavuudesta, hänen ei pidä hyväksyä virheellisesti tai puutteellisesti toimivaa ohjelmaa yksikön käyttöön.
Tiedon omistajalla on valtuus tarkastuttaa kehitystyön menetelmät ja tuotantotoiminnan menettelyt. Omistajavastuut on syytä olla kirjalliset. Pohdi kenen tehtävänä on yrityksessäsi varmistaa ulkoa ostetun tuotantotoiminnan luottamuksellisuutta?

Tietojärjestelmän kehittäminen

Järjestelmiä suunnittelee organisaation oma ja ulkopuolinen henkilöstö, suuri joukko ihmisiä. Perusasiana on varmistaa henkilöiden luotettavuus ja arvioida työtehtävän luottamuksellisuus. Hyvänä käytäntönä on selkiyttää jokaiselle vaitiolositoumuksen ja salassapidon

merkitys. Järjestelmäkehitysprojektissa projektipäällikkö varmistaa, että jokainen on ymmärtänyt vastuunsa ja muut henkilöstöhallinnolliset asiat ovat järjestetty.

Projektipäällikön tehtävänä on varmistaa, että

- toiminnan tuntevien henkilöiden työpanos on riittävä, ja että määrittely vastaa käyttäjän tarpeita.
- jo varhaisessa vaiheessa päätetään, millaisista tietojen ylläpidoista halutaan kerätä lokitietoa ja miten se teknisesti on turvallista ja toimiva
- suunnitellaan toiminta- ja virhelokit erikseen
- ohjelman muutostarpeiden vaikutukset arvioidaan ennen muutosta ja hyväksytetään ne tiedon omistajalla
- kriittisten ja tärkeiden tietojen syöttö-, käsittely- ja tuloskontrollit ovat riittävät ja, että ne takaavat tiedon eheyden ja luottamuksellisuuden
- käytettävät omat ja ulkopuolisen alihankkijan työvälineet ja -kaluohjelmistot on listattu ja niiden käyttötavoista ja -ympäristöistä on sovittu tiedon omistajan kanssa
- kaikki tuotantotietojen korjaukset, kopioinnit, lähetykset, muut ajot, kyselyt, listaukset, joissa tarvitaan työkaluohjelmia lokataan ja varmistetaan jälkikäteen tapahtuneen tarpeellisuus
- ohjelman testaaminen suoritetaan eri ympäristössä kuin missä on yrityksen tuotantotiedot, kuten asiakas-, hinta-, laskutus-, tuotekehitys-, palkka- ja terveystiedot
- kaikki paperilla oleva testausaineisto tuhotaan turvallisesti ja testitunnukset poistetaan käyttäjiltä
- ohjelman / sovelluksen toiminta dokumentoidaan
- ohjelmamuutosten hallinta, kuten testausympäristö, -menet-telyt, tuotantoonottomenettelyt, noudattaa yhtiön omia ja alihankkijan standardeja ja määräyksiä.

Vastuiden selkiyttämiseksi on hyvä tehdä projektipäällikölle muistilista. Tekninen suunnittelu vastaa siitä, että *ohjelma toimii luotettavasti* ja sen käsittelysäännöt ovat oikeat sekä siitä, että tiedon käsittely ja kulku on jälkikäteen tarkastettavissa.

Tietojärjestelmän tuotanto

Yrityksen tietojenkäsittelyn toiminnan jatkuvuuden kannalta perusasiana on sopia näistä asioista kirjallisesti alihankkijan kanssa ja tutustua molemmin puolin toistensa toimintaan sekä tarkastaa palvelua tarjoavan yrityksen toimintatavat. Henkilöiden luotettavuus ja ammattitaidosta huolehtiminen ovat elintärkeitä molemmille osapuolille.

Tietohallinnon ja palvelukeskuksen vastuulla on huolehtia siitä, että

- yrityksen tietojenkäsittelyn erilaisiin häiriö- ja poikkeamatilanteisiin on varauduttu ennalta suunnitelluin menettelyin ja suunnitelmin sekä tositilanne harjoituksin
- tiedot on varmistettu ja niiden tuoreet suojakopiot saatavilla tarvittaessa
- järjestelmiä käytetään henkilökohtaisten käyttäjätunnuksin, joihin on liitetty kuukausittain vaihtuvat salasanat, joiden pituus on minimissään 6 merkkiä ja merkkeinä kirjaimia ja numeroita
- uusien ohjelmaversioiden tuotantoonottomenetelmät takaavat ohjelmaversion eheyden
- kaikki tuotantotietojen muuttaminen, kopiointi, siirtäminen ja tuotanto-ohjelmien tuotantoonotot ja käynnistämiset lokataan
- lokeilta tuotetaan raportit tietojen omistajille ja tuotantotoiminnasta valvonnasta vastaavalle yrityksen edustajalle.

Sopimuksiin tietoturvavaatimukset alihankkijoille ja partnereille

Vaikka tuotanto on ulkoistettu, vastuu tietojen oikeellisuudesta ja palvelun toimivuudesta sekä juridiset vastuut ovat yrityksellä itsellään. Tärkeää on erottaa käyttäjäyksikön eli tiedon omistajan, tietojärjestelmäsuunnittelun, tietohallinnon ja ulkoistetun tietohallinnon roolit ja tehtävät tietoturvallisuuden luomisessa ja ylläpitämisessä. Sopimusta tehtäessä on syytä pohtia, miten myös suuren kehitysprojektin riskit arvioidaan.

Sen yksikön johdon, joka tekee ja allekirjoittaa palvelukeskusten tai muiden alihankkijoiden kanssa sopimukset, vastuulla on huolehtia, että yllä mainitut tehtävät ovat mukana keskinäisissä sopimuksissa otsikoin ‘Yrityksen tietoturvavaatimukset ja palvelun tarjoajan tietoturvamenettelyt’ ja että sovittujen menettelyjen tarkastusoikeutta käytetään.

Laadukas tietoturvallisuuden hallintajärjestelmä ohjaa ja osaltaan varmistaa eri osapuolten vastuut ja tehtävät. Tämä on monen vuoden työn tulos, joka vaatii niin asioiden kuin ihmisten johtamista.

Tuija Kyrölä,
Tietoturvakonsultti,
TietoTurvaKoulutus Oy
p. 09-586 1650,
gsm. 040-545 5465
email: tuija.kyrola@kolumbus.fi