v. 0.4

EVASERVE

Moduuli:
Tietopalveluiden tietoturvana arviointi

http://www.evaserve.fi

Muutoshistoria

Versio	*Päiväys*	*Tekijä*	*Kommentteja*
0.1	8.6.2005	Arto Laikari	Ensimmäinen draft-versio. Moduulin rungon hahmottelu.
0.2	30.6.2006	Jani Suomalainen	Muokattu arviointiprosessin rakennetta; lisätty tekstiä
0.3	21.9.2006	Jani Suomalainen	Pieniä lisäyksiä
0.4	27.11.2006	Jani Suomalainen	Pieniä lisäyksiä
0.5	7.2.2007	Jani Suomalainen	Pieniä muutoksia

Sisällysluettelo

1 Johdanto

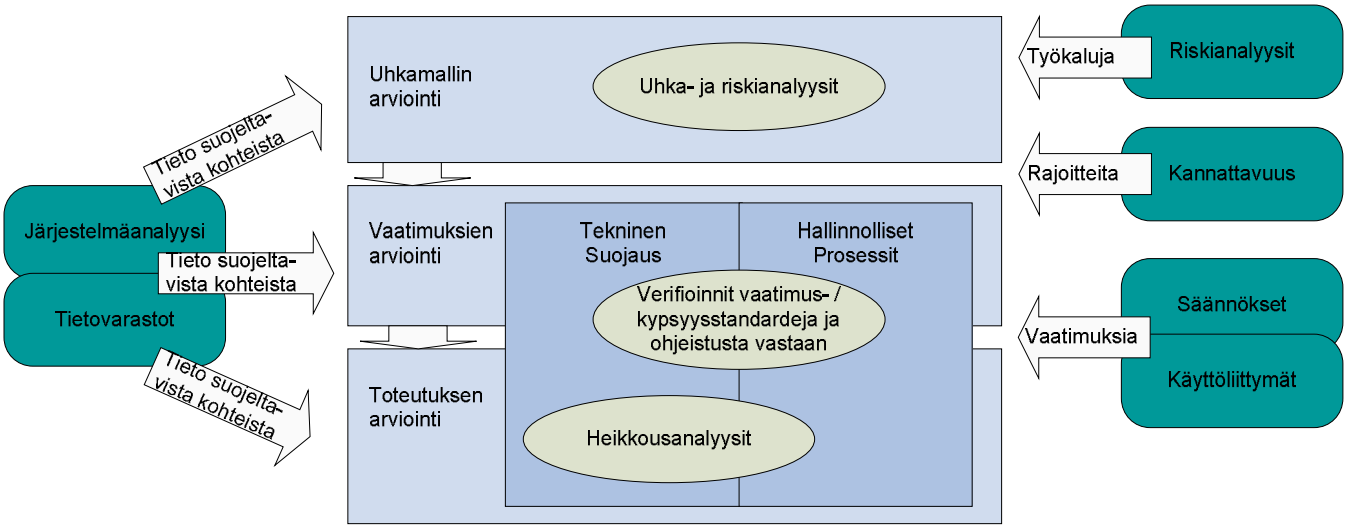
Tietopalveluiden toiminnan varmuus ja käyttöoikeuksien kontrollointi vaativat vahvojen tietoturvamekanismien käyttöä sekä koko järjestelmän kattavaa tietoturvauhkat huomioivaa suunnittelua ja toteutusta. Tässä arviointimoduulissa esitellään ja listataan parhaita käytäntöjä ja menetelmiä, joita voidaan käyttää arvioitaessa tietopalveluhankkeen, -järjestelmän tai -palvelun tietoturvan riittävyyttä ja laatua. Dokumentissa käsitellään tietoturvan arviointiin liittyviä eri osa-alueita esittelemällä vaihtoehtoisia menetelmiä, standardeja ja tarvittavaa ohjeistusta. Dokumentti pyrkii myös tuomaan esille VTT:n osaamista ja referenssejä. Arviointimenetelmiä voidaan käyttää kaikenlaisten tietojärjestelmien ja telematiikkahankkeiden arviointiin.

2 Arviointiprosessi

Tietoturva-arviointien lähtökohdat ovat erilaisia. Arviointi voidaan tehdä hankkeen suunnittelu-, toteutus- tai käyttövaiheessa. Ihanteellisessa tapauksessa tietoturva huomioidaan jo hankkeen suunnitteluvaiheessa, jolloin se tukee hankkeen toteutusta ja käyttöönottoa. Tietoturvaparannusten tuonti jo toteutettuun ja käytössä olevaan järjestelmään on yleensä vaikeampaa. Arvioinnin laajuus ja syvyys riippuvat käytettävissä olevista resursseista.

VTT on osallistunut useisiin yksittäisien tietoturvamittareiden ja tuotteiden tietoturvan kehitys- ja evaluointiprojekteihin. Tämän lisäksi VTT on panostanut tietoturvakokonaisuuksien analysointiin tutkimalla tietoturvan mittaamiseen liittyviä menetelmiä ja käytäntöjä. Esimerkiksi VTT:llä on tehty tutkimus [1] Suomessa yleisesti teollisuus- ja julkisen sektorin käytössä olevista tietoturvan mittaus- ja evaluointiprosesseista. Lisäksi VTT:llä on pyritty määrittelemään tietoturvakokonaisuuksien evaluointiprosessia tietoturvatodisteiden keräämisen näkökulmasta [2].

Tietopalvelujen tietoturvan arviointiprosesseja voidaan tarkastella Kuva 1:ssä esitetyn mallin mukaisesti. Tietoturva-analyysit lähtevät suojattavien resurssien määrittämisestä, näihin liittyvien uhkien tunnistamisesta ja riskianalyysien perusteella tehtävästä oleellisten uhkien priorisoinnista. Tämän jälkeen uhkista määritellään tietoturvavaatimuksia, joiden toteuttaminen vaatii usein sekä teknisten suojausmenetelmien käyttö että hallinnollisten prosessien tukea. Sekä vaatimuksia että toteutusta voidaan arvioida käyttämällä hyväksi olemassa olevia evaluointistandardeja, jotka ohjeistavat parhaista käytännöistä tarjoamalla arviointipuitteita ja tarkistuslistoja. Toteutuksista voidaan lisäksi pyrkiä etsimään tyypillisiä suunnittelu- ja toteutusheikkouksia erilaisilla analyysimenetelmillä ja työkaluilla. Kuvassa on esitetty myös tietoturvan arviointimoduulin suhde muihin arviointimoduuleihin, jotka on esitetty vihreillä laatikoilla.



Kuva 1. Tietoturvan arvioinnin osa-alueet ja liitynnät muihin moduuleihin

Arviointiprosessin korkean tason tehtävät on kuvattu vaiheittain Taulukko 1:ssä. Prosessi ei ole täysin suoraviivainen vaan eri vaiheista voidaan tarvittaessa palata aikaisempiin vaiheisiin.

Taulukko 1. Arviointiprosessin tehtävät

Tehtävän nimi	Tehtävän kuvaus
1 Tietoturvakriittisten resurssien ja osien identifiointi ja rajaus	Kerätään suojeltavista resursseista ja arkkitehtuurista tietoa, joka mahdollistaa uhkamallin ja toteutuksen arvioinnin
1.1 Tietoteknisen arkkitehtuurin selvittäminen	Selvitetään ja hahmotellaan järjestelmän arkkitehtuuri, jossa kuvataan rakenneosat, käyttäjät, toimijat, tietoliikenneyhteydet, sekä järjestelmän toiminnallisuus
1.2 Arvioinnin laajuuden määrittely ja suunnittelu	Määritellään, kuinka laajasti ja tarkasti arviointi toteutetaan. (Sisältää määrittelyn, mitkä osat järjestelmästä arvioidaan, jos koko järjestelmää ei arvioida). Tehdään vaatimusmäärittely arvioinnille ja sen pohjalta luodaan arviointisuunnitelma
2 Uhkamallin arviointi	
2.1 Uhka-analyysit	Identifioidaan järjestelmään kohdistuvat tietoturvauhkat
2.2 Riskianalyysit	Arvioidaan uhkien toteutumisen todennäköisyys ja seuraukset. Tämän tiedon perusteella voidaan valita uhkat, jotka pitää torjua
3 Vaatimusten ja toteutuksen arviointi	
3.1 Vaatimusten vertailu torjuttaviin uhkiin	Tarkistetaan, että oleelliset uhkat on kirjattu järjestelmän tietoturvavaatimuksiksi
3.2 Vaatimusten vertailu teknisiin ja hallinnollisiin ohjeistuksiin	Verrataan tietoturvavaatimuksia kirjallisuudessa olemassa oleviin referenssivaatimuslistoihin
3.3 Toteutuksen vertailu järjestelmän vaatimusmäärittelyihin	Verrataan teknistä toteutusta ja hallinnollisia prosesseja järjestelmän omiin tietoturvavaatimuksiin
3.4 Toteutuksen vertailu teknisiin ja hallinnollisiin ohjeistuksiin	Verrataan teknistä toteutusta ja hallinnollisia prosesseja yleisiin ja hyväksi havaittuihin referenssikäytäntöihin.
3.5 Heikkousanalyysit	Arvioidaan valitut arviointisuunnitelmassa määritellyt osa-

	alueet valittuja menetelmiä ja työkaluja käyttäen
4 Yhteenveto ja raportointi	Laaditaan syntyneestä materiaalista arviointiraportti

3 Tietoturvakriittisten resurssien ja osien identifiointi ja rajaus

Tietoturvan arviointi edellyttää järjestelmän toiminnallisuuden, kokonaisarkkitehtuurin ja uhkien ymmärtämistä. Ensimmäisessä vaiheessa on tietoturvan kannalta oleellista tunnistaa resurssit (assets) ja määritellä, kuinka laajasti ja tarkasti arviointi toteutetaan.

Tietojärjestelmistä selvitetään järjestelmän toiminnallisuus ja arkkitehtuuri, jossa kuvataan muun muassa rakenneosat, käyttäjät, roolit, toimijat, tietoliikenneyhteydet, rajapinnat, tietovirrat. Tietoa voidaan kerätä eri tavoin kuten kysymyslomakkeilla, haastatteluilla, järjestelmäkuvausdokumenttien avulla ja mahdollisesti teknisten työkalujen avulla. Tarvittaessa apuna voi käyttää ***järjestelmäanalyysi-*** sekä ***tietovarastot-moduulien*** pohjalta tehtyjä analyysejä.

Arvioitavana voi olla hanke, järjestelmä, suunnitelma, toteutus tai käyttö. Joissakin tapauksissa voidaan pyrkiä koko organisaation toimintatavan kehittämiseen kun taas joissakin tapauksissa keskitytään vain teknisiin tai tiettyyn ohjelmistotuotteeseen liittyviin kysymyksiin tai tietystä suunnasta tulevien uhkien torjumiseen. Esitellyistä menetelmä- ja käytäntöalueista voidaan valita tilanteeseen sopivat tehtävät.

4 Tietoturvauhka- ja riskianalyysit

Uhka-analyysin haasteena on mahdollisimman kattava uhkien tunnistaminen kaikista olemassa olevista uhkista. Kohteen uhkien määrittely perustuu ymmärrykseen sekä arvioitavasta järjestelmästä että tyypillisistä tietoturvauhkista. Usein käytettävä keino uhkien etsimisessä on järjestää ns. aivoriihi. Näihin kokouksiin osallistuvat sekä tuotteen tuntevat kehittäjät, jotka usein myös vastaavat tietoturvan toteuttamisesta, sekä tietoturvaevaluoijat, jotka ohjaavat kokouksen kulkua. Kehittäjien osallistuminen uhkien määrittelyyn sitouttaa ja näin lisää todennäköisyyttä, että havaittuja ongelmia todella korjataan. Kehittäjät mukaan ottava uhkamäärittelyprosessi voi koostua esimerkiksi seuraavista vaiheista [3]:

1. Tuotteen tietovirtojen kuvaus kehittäjien toimesta mahdollistaa etukäteisvalmistelut
2. Tietoriihissä kehittäjät tunnistavat uhkia tietoturvan erityisosaajan ohjauksessa
3. Uhkadokumentin valmistaminen
4. Uhkadokumentin tarkistuskokous
5. Uhkien vertaisvarmennus
6. Korjaavat toimenpiteet

Tietoturvauhkien etsimisessä voidaan käyttää hyväksi kirjallisuudesta löytyviä esimerkkiuhkia ja kategorioita, joihin tyypillisimmät uhkat liittyvät. Luokittelu helpottaa tietoturvatilanteen ymmärtämistä ja auttaa oleellisten uhkien systemaattisessa etsimisessä ja puolustuskeinojen valinnassa. Uhkien luokittelu voi perustua esimerkiksi:

- Resurssiin tai järjestelmän osaan, johon hyökkäykset kohdistuvat tai joiden kautta hyökkäykset toteutuvat
- Hyökkäysparadigmaan eli tapaan, jolla tunkeutuminen tai vahinko aiheutetaan. Esimerkiksi hyökkäyssuunnat voidaan jakaa haittaohjelmien, ulkoverkoista tulevien ja sisäisten käyttäjien aiheuttamiin kategorioihin.

- Hyökkäyksen seuraukseen mistä esimerkkinä on CIA malli (luottamuksellisuus, muuttamattomuus, saatavuus – confidentiality, integrity, availability), joka on laajalti käytetty suuren osan uhkista kattava luokittelutapa ja jonka pohjalta on helppo määritellä vaatimuksia puolustusmenetelmiksi. Toinen esimerkki hyökkäyksien seuraukseen perustuvasta mallista on Taulukko 2:ssä esitetty STRIDE [4] malli.

Taulukko 2. STRIDE [4] uhkien luokittelumalli

Uhkakategoria	*Kuvaus*
Väärän identiteetin käyttö (Spoofing)	Käyttämällä väärää identiteettiä, esimerkiksi varastettuja tai väärennettyjä tietoja, hyökkääjä voi päästä kirjautumaan palveluun.
Tiedon muokkaaminen (Tampering)	Tiedon luvaton muokkaaminen voi tapahtua joko sitä siirrettäessä tai sen ollessa talletettuna
Toimien kiistäminen (Repudiation)	Toimet ja tapahtumat voidaan kiistää, ellei niistä jää luotettavia jälkiä.
Tiedon paljastaminen (Information disclosure)	Tiedon paljastaminen viittaan esimerkiksi tiedon luvattomaan käyttöön tai sen luvattomaan kopiointiin ja levitykseen.
Palvelun esto (Denial of service)	Palvelun esto hyökkäykset voivat tapahtua infrastruktuuri-, laite- tai sovellustasolla. Esimerkiksi palvelimen pommittaminen pyynnöillä tai standardin vastaisesti muotoillut viestit ovat mahdollisia tapoja hyökätä palvelun saatavuutta vastaan.
Oikeuksien lisäys (Elevation of privilege)	Oikeuksien lisäämishyökkäyksillä käyttäjä hankkii oikeuksia, joita tarvitaan muiden hyökkäyksien toteuttamiseen.

Kaikkia havaittuja uhkia ei välttämättä torjuta. Puolustuskeinojen toteuttamisessa pitää myös huomioida panostukset, joita puolustuskeinoihin käytetään sekä uhkien esiintymistodennäköisyydet ja -vaikutukset.

Riskianalyyseilla selvitetään uhkien toteutumisen todennäköisyydet ja kustannukset. Riskianalyyseissä käytettäviä menetelmiä on käsitelty yleisemmin ***riskianalyysimoduulissa***. Tietoturvaspesifisien riskien hallintaa on käsitelty esimerkiksi **NIST 800-30** [5] ohjeistuksessa. Dokumentti käsittelee uhkien tunnistamismenetelmiä, riskien hallintaa ja riskejä ehkäiseviä menetelmiä yleisellä tasolla. NIST on tuottanut myös muita tietoturvan parhaiden käytäntöjen oppaita [6].

Tietoturvapuolella yleinen tapa analysoida riskejä on hyökkäyspuiden (attack trees) [7] käyttäminen. Hyökkäyspuut mahdollistavat hyökkäysten eri vaiheiden ja vaiheiden suhteiden havainnollistamisen ja graafisen dokumentoinnin. Mahdollisia ongelmia ovat niiden luomat harhat formaalista kaikkien uhkien kartoittamisesta sekä työläys.

Tietoturvariskien analysointiin, hallintaan ja vähentämiseen liittyviä VTT:n projekteja ovat esimerkiksi IRRIIS (IST/Integrated Risk Reduction of Information-based Infrastructure Systems), SHOPS (EUREKA/Smart Home Payment Systems) ja ANSO (ITEA/Autonomic Networks for SOHO users). Ensimmäisessä on analysoitu energian jakelu ja telekommunikaatioverkkoihin, toisessa maksujärjestelmiin liittyviä riskejä ja kolmannessa heterogeenisten kotiverkkojen tietoturvauhkia.

5 Vaatimuksien ja toteutuksen arviointi

Tietopalvelun vaatimuksien ja toteutuksen tietoturvallisuuden arvioinnit tehdään suunnittelu ja toteutus dokumenttien sekä koodin katselmoinneilla ja analyyseillä. Arvioinneissa tarkistetaan että kaikki

tunnistetut ja oleellisiksi arvioidut uhkat huomioidaan sekä vaatimusmäärittelyissä että toteutuksessa. Lisäksi arvioinneissa voidaan käyttää olemassa soveltuvia ohjeistuksia ja referenssitarkastuslistoja.

5.1 Teknisen suojauksen arviointi

Tietopalvelun tietoturvan luotettavuuden ja vahvuuden arviointi riippuu siinä käytettävistä komponenteista kokonaisuuden ollessa yleensä yhtä vahva kuin sen heikoiten suojattu osa. Tietoturvaa tarkastellaan koko järjestelmän toteutuksen ja toiminnan kannalta, mutta arviointia varten koko järjestelmän tietoturva voidaan jakaa pienempiin paremmin hallittaviin osakokonaisuuksiin. Esimerkiksi yksi mahdollisuus on jakaa tietoturvallisuus viiteen alijärjestelmään [8]: seuranta (auditointi), eheys (integriteetti), käytönvalvonta, tietovirtojen kontrollointi ja identiteettien hallinta.

Yksittäisiä komponentteja analysoitaessa voidaan käyttää sopivia tietoturvavaatimusmäärittelyjä. Esimerkiksi **Common Criteria** (CC) standardia [9] käytetään yleisesti tietoturvan evaluoinnissa. CC tarjoaa kehyksen, jonka avulla voidaan määritellä erilaisia tietoturvavaatimuksia yksittäisille tuotteille ja vaatimusprofiileja tuoteperheille. CC:n soveltaminen on kuitenkin työlästä minkä takia standardia on käytetty pääasiassa suhteellisten pienien tietoturvakriittisten tuotteiden kuten älykorttien evaluointiin. Tietoturvaprofiileja on kuitenkin määritelty myös esimerkiksi palomuureille ja tietokantaohjelmistoille.

Tyypillisin tietoturvan luotettavuuden mittari on laajan julkisen tarkastelun ja käytön tuoma kokemus ja maine menetelmän tai ohjelmiston murtamattomuudesta ja käytettävyydestä. Tämä mittari soveltuu erityisesti oikeuksien hallintamenetelmiä ja salausalgoritmeja arvioitaessa. Uusien kokeilemattomien ratkaisujen arvioinneissa voidaan käyttää muita maineeseen perustuvia todisteita [2]:

- Tekijän (esimerkiksi ohjelmiston toimittajan) työkäytännöt
- Tekijän muiden töiden maine
- Laatu- ja tietoturvastandardien käyttö
- Ulkopuolisten tekemät arvioinnit tekijästä ja arvioijien maine

Muita esimerkkejä tietoturvamittareista ovat:

- Käytettävyysvaikutuksia voidaan arvioida laskemalla tarvittavien käyttäjän interaktioiden määrä. Käyttäjätutkimuksilla voidaan lisäksi selvittää mahdollisien tietoturvaheikkouteen johtavien käyttäjän toimien määrä ja yleisyys.
- Salausalgoritmien vahvuuden arviointiin voidaan käyttää matemaattisia kompleksisuusteorioita. Tällöin turvallisiksi luokitellaan vain epärealistisilla resursseilla murrettavat tai murtamattomina pidetyt menetelmät.
- Käytettyjen, saamaa uhkaa torjuvien, menetelmien määrä mittaa tietyissä tapauksissa järjestelmän vahvuutta yksittäisiä heikkouksia vastaan. Yksittäinen tieturva-aukon aiheuttamaa uhkaa koko järjestelmän murtamisesta kerralla voidaan pienentää useilla päällekkäisillä tietoturvamenetelmillä. Käytännössä kaikki yksittäiset tietoturvamenetelmät ovat kierrettävissä tai murrettavissa, jos resursseja on tarpeeksi käytössä. Tämän takia useiden menetelmien käyttö voi lisätä hyökkääjien tarvitsemia resursseja.
- Saatavuuden suojausta voidaan arvioida esimerkiksi virheiden sietokykyä lisäävien menetelmien kuten redundanssin käytön määrällä.

5.2 Heikkousanalyysit

Monet toteutuksissa olevat tietoturvaheikkoudet paljastuvat usein vasta käytön kautta. Tuotteet, teknologiat ja käytännöt, jotka ovat olleet käytössä useampia vuosia, ovat koetellumpia ja monet niissä ol-

leista heikkouksista on karsittu. Heikkouksia voidaan kuitenkin pyrkiä etsimään myös etukäteen erilaisilla testaukseen ja koodin analysointiin perustuvilla menetelmillä.

Tietoturvan käytännön vahvuuden testauksessa voidaan käyttää kokeneita testauksen ja tietomurtojen osaajia - hakkeritiimejä. Nämä testaajat kokeilevat erilaisia tunnettuja hyökkäyksiä vaihtelevilla parametreilla tarkoituksenaan löytää heikkouksia, joita myös oikeat hyökkääjät voisivat käyttää hyödykseen. Yksittäisten tuotteiden ja ohjelmistokomponenttien, erityisesti verkkosovellusten, tietoturvatestaamista varten on olemassa työkaluja, jotka automatisoivat hyökkäyksien tekoa. Esimerkiksi VTT on osallistunut Protos-työkalun [10] kehittämiseen. Työkalulla voidaan generoida suuri määrä erimuotoisia viestejä, joiden avulla on mahdollista paljastaa heikkouksia verkkopalvelimista.

Ohjelmistovirheet ovat tärkeä yksittäinen syy tietoturvaongelmiin. Potentiaalisia virheitä voidaan etsiä käymällä ohjelmakoodia läpi joko koodin katselmointien avulla tai käyttämällä staattisia ja dynaamisia analyysityökaluja. Automaattisten työkalujen ongelmana on niiden epätarkkuus ja tietoturvan arvioiminen ohjelmistovirheitä etsimällä on työlästä. Ohjelmien toimintaa voidaan myös pyrkiä verifioimaan formaaleilla menetelmillä, joilla ohjelman virheetön toiminta pyritään matemaattisesti todistamaan. Ohjelmien formaali mallintaminen on kuitenkin työlästä eivätkä nämä menetelmät sovellu monimutkaisten ohjelmistojen luotettavuuden arviointiin.

5.3 Turvaprosessien arviointi

Yksittäisten teknisten ratkaisujen lisäksi palvelujen tietoturva koostuu hallinnollisista toimista kuten ohjeistuksesta, koulutuksesta, CERT:in ja valmistajien haavoittuvuustiedotusten seurannasta, ohjelmistojen päivityksestä sekä toimista uhkien toteutuessa. Kokonaistietoturvaan on olemassa standardeja, joiden soveltuvien osien yhteensopivuutta tietopalvelun kanssa voidaan arvioida.

ISO 17799 (BS 7799) standardi [11] määrittelee ohjeistuksen kokonaistietoturvallisuuden hallinnoinnille. Standardi koostuu kymmenestä osa-alueesta:

1. Tietoturvapolitiikka (security policy)
2. Turvallisuusorganisaatio (security organization)
3. Tietovarastojen vastuuttaminen ja omistajuus (assets classification and control)
4. Henkilöstöön liittyvät tietoturvariskit (personnel security)
5. Fyysinen ja toimintaympäristön turvallisuus (physical and environmental security)
6. Tietojärjestelmänverkon hallinta (computer and network management)
7. Järjestelmään pääsyn valvonta (system access control)
8. Tietojärjestelmän kehittäminen ja ylläpito (systems development and maintenance)
9. Liiketoiminnan jatkuvuutta uhkaavien riskien hallinta (business continuity planning)
10. Lakisääteisten ja muiden vaatimusten huomioon ottaminen (compliance)

Muita tieturvan hallinnointiin liittyviä evaluointistandardeja ovat:

- SSE-CMM (Systems Security Engineering Capability Maturity Model, ISO/IEC 21827) [12] standardi määrittelee ja ohjeistaa tietoturvaprosessien kypsyyden arvioimisen.
- INFOSEC IA-CMM
- IS Program Maturity Grid
- Murine-Carpenter SW Security Metrics

VTT:llä on kehitetty ja käytössä pienille ja keskisuurille yrityksille tarkoitettu evaluointimenetelmä – **ketterä tietoturvan hallintajärjestelmän kehitysmenetelmä** [13]. Menetelmä on ISO 17799 yhteensopiva tapa kehittää yrityksen tietoturvaprosesseja. Menetelmään kuuluvat seuraavat vaiheet: palaveri

johdon kanssa, tietoturvapolitiikka, strateginen turvallisuus (henkilöstö ja fyysinen turvallisuus), operatiivinen turvallisuus, jatkuvuussuunnittelu, ohjeet, koulutus ja mittaaminen. Menetelmää on käytetty esimerkiksi EUREKA/SHOPS projektin yhteydessä.

6 Raportointi

Arvioinnin tulokset voidaan esittää kirjallisena raporttina. Raportista selviää arvioinnissa läpikäydyt tietopalvelun osat, arvioinnin vaiheet sekä käytetyt menetelmät ja standardit. Tuloksia voivat olla esimerkiksi havaitut heikkoudet tai poikkeamat yleisesti hyväksyttyihin käytäntöihin nähden sekä jäännösriskit, eli torjumattomien uhkien vaikutukset ja todennäköisyydet. Tämän lisäksi raportissa voidaan listata ja suositella mahdollisia korjaustoimia.

Lähdeluettelo

1 Jorma Kajava, Reijo Savola. Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes. The European University Information Systems Conference (EUNIS). 2005.
2 Reijo Savola, Juha Röning. Towards Security Evaluation based on Evidence Information Collection and Impact Analysis. The International Conference on Dependable Systems and Networks (DSN-2006). 2006.
3 Peter Torr. High-Level Threat Modelling Process. Microsoft. blogs.msdn.com/ptorr/archive/2005/02/08/368881.aspx
4 J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla, Anandha Murukan. Improving Web Application Security: Threats and Countermeasures. Microsoft. 2003. msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/THCMCh02.asp
5 Gary Stoneburner, Alice Goguen, Alexis Feringa. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. Special Publication 800-30. 2002. csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
6 NIST Computer Security Special Publications. National Institute of Standards and Technology. csrc.nist.gov/publications/nistpubs/index.html
7 Bruce Schneier. Modeling Security Threats: Attack Trees. Dr. Dobb's Journal. 1999. www.schneier.com/paper-attacktrees-ddj-ft.html
8 J.J. Whitmore. A method for designing secure solutions. IBM Systems Journal, vol 40, no 3, 2001.
9 Common Criteria. www.commoncriteriaportal.org
10 Rauli Kaksonen. A functional method for assessing protocol. Implementation security. VTT Technical Research Centre of Finland. VTT Publications : 448. 2001. www.vtt.fi/vtt_show_record.jsp?target=julk&form=sdefe&search=42220.
11 International Organization for Standardization. ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management. www.iso.org/iso/en/prods-services/popstds/informationsecurity.html.
12 SSE-CMM home page. www.sse-cmm.org/index.html.
13 Jarkko Holappa, Timo Wiander. PK-Yrityksen Tietoturvakehikko. Ketterä tietoturvan hallintajärjestelmän kehitysmenetelmä. 2006.