Yrityksen verkkopalveluiden turvallisuuden varmistaminen sovellusten riskienhallinnalla ja auditoinnilla.

11. Turvallisuusjohdon
koulutusohjelma
Aalto-yliopiston teknillinen
korkeakoulu
Koulutuskeskus Dipoli
Tutkielma 1.3.2011
Pekka Haapala

SISÄLLYSLUETTELO

1.	**Johdanto**		**3**
	1.1.	Tutkielman tavoitteet	3
	1.2.	Tutkielman rajaukset	4
2.		**Tutkimuksen ongelma ja viitekehys**	**4**
3.		**Käsitteistö**	**5**
	3.1.	OWASP	5
	3.2.	Sovelluksen tietoturvariskit	6
	3.3.	Käyttötapaukset	7
	3.4.	Väärinkäyttötapaus	7
	3.5.	Haavoittuvuus	7
	3.6.	Tietoturvakontrolli	7
	3.7.	Vaatimusmäärittely	10
4.		**Riskienhallinta**	**11**
5.		**Auditoinnit**	**13**
	5.1.	Yleisiä Tietoturva-auditoinnilla saatavia hyötyjä	13
	5.2.	Tietoturva-auditoinnin aiheuttamia riskejä	14
	5.3.	Auditointien tuloksia	15
6.		**Johtopäätökset**	**16**

1. Johdanto

Tietoturvallisuusriskit ja -tilanne tulisi tuntea yrityksissä nykyistä paremmin. Vaikka yritysten palvelimet olisi rakennettu huolella turvallisiksi, tietoa käsitellään työasemissa, jotka ovat WWW-selaimineen aivan liian haavoittuvia.

Automaattiset seurantajärjestelmät eivät lähtökohtaisesti kykene tunnistamaan kohdistettuja tietokaappauksia, koska niitä ei tehdä tunnetulla hyökkäys-sormenjäljellä vaan normaalia käyttöä mukaillen.

Toimintaympäristön haavoittuvuuteen tulisi kiinnittää yrityksissä enemmän huomiota. (Keskusrikospoliisi, rikostietopalvelu, 7.10.2009, Arkistoviite KRP/RTP 5230/213/09)

Painopiste yleisesti Tietoturvapanostuksissa on teknisen ympäristön kehittämisessä, verkkosovelluksiin liittyvät riskit jäävät usein huomioimatta ja tunnistamatta. OWASP Helsingin kommentoimana:

Liiketoiminnan siirtyessä verkkoon, yhä suurempi paino on verkkosovellusten riskeissä. Tietoturvallisuuden nykyinen opetus ja tutkimus suomalaisissa oppilaitoksissa ei kokemustemme mukaan vastaa tämän päivän ohjelmistokehityksen, ja sitä kautta liiketoiminnan tarpeita. (www.owasp.org/index.php/Helsinki)

1.1 Tavoite

Tutkielman tavoitteena on esitellä yksinkertainen malli, mitä hyödyntämällä saadaan riskienhallinnan keinoin löydettyä sovellusten kriittiset pisteet verkkosovellusten tietoturvallisuuden varmistamiseksi.

1.2 Rajaus

Tutkielmassa ei määritellä riskin käsitettä tai kuvata yrityksen riskienhalllintaprosessia yleisellä tasolla. Yleisenä viitekehyksenä yrityksen riskienhallintaan voidaan pitää Elinkeinoelämän keskusliiton Yritysturvallisuus kaaviota, jonka yhtenä osatekijänä Tietoturvallisuus. Tietoturvallisuuteen liittyvästä riskienhallinnasta on tarkemmin määritelty esimerkiksi Valtionvarain ministeriön Vahti –ohjekokoelmassa.

Riskien kuvaaminen ja riskienhallinta keskittyy verkkosovelluskehityksen tietoturvan näkökulmasta käsiteltäviin riskeihin.

2. Tutkimuksen ongelma ja viitekehys

Tutkimuksen ongelma keskittyy verkkosovelluksen riskienhallintaan, tietoturva-kontrollien määrittelyyn verkkosovellusten ja verkkopalveluiden sovelluskehityksen yhteydessä tapahtuva vaatimustenmukaisuuden todentaminen vaatimusmäärittelyn, riskien tunnistamisen, tietoturvakontrollien määrittelyn toteutuksen, testauksen ja auditointien avulla.

Yleisesti IT riskienhallinta ei tunnista sovelluksissa olevia riskejä, perinteinen riskienhallinta keskittyy teknisen ympäristön toiminnan varmistamiseen sekä jatkuvuuden varmistamiseen. Sovellushankkeissa riskienhallinta keskittyy hankkeen läpiviennin riskeihin eikä riskeihin, joita hankkeessa rakennettava sovellus tuo mukanaan.

Tässä työssä ei syvällisemmin paneuduta yleiseen riskien määrittelyyn tai riskien hallinnan toteutukseen yrityksessä ja ei käytä läpi yleisesti tietotekniikkaan, tietotekniikka liiketoimintaa liittyvää riskienhallintaa.

3 Käsitteistöä

3.1 Verkkosovellus

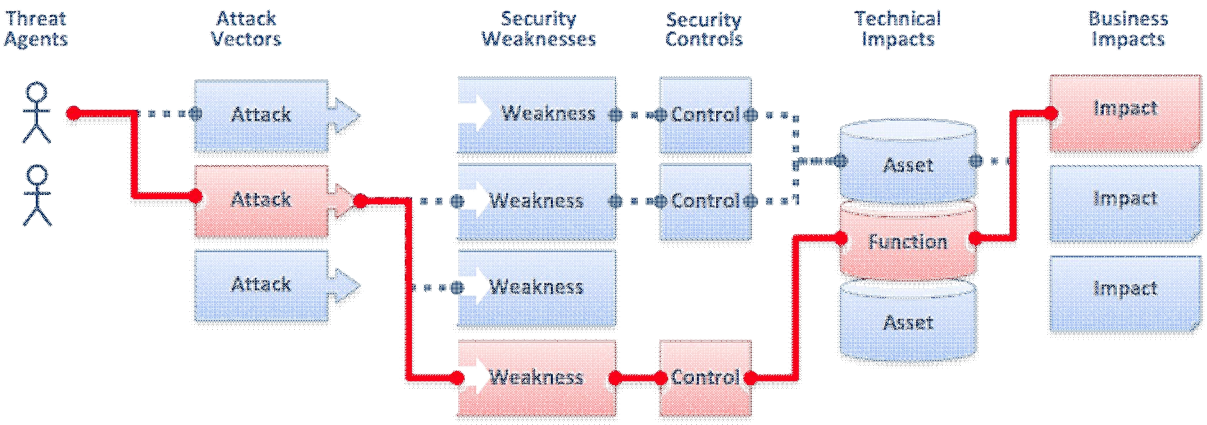
Tässä yhteydessä käytetään verkkosovellus, myöhemmin myös sovellus termiä kuvaamaan Web palvelun käyttöä varten rakennettua ohjelmistokokonaisuutta, jolla pyritään tarjoamaan erityyppisiä kauppa, pankki, informaatiopalveluita loppukäyttäjille.

3.1 OWASP

Verkkosovelluksien tietoturvaan keskittyneen, kansainvälisen vapaaehtoisjärjestö OWASP:n (Open Web Application Security Project) tarkoituksena on edesauttaa turvallisten sovellusten kehitystä ja ylläpitoa. Järjestö on voittoa tavoittelematon ja se toimii jo lähes sadassa maassa. Suomen OWASP Helsinki Chapter -niminen alajaos perustettiin 2000-luvun puolivälissä.

3.2 Mitä ovat sovelluksen tietoturvariskit

Sovelluksen käyttäjä voi käyttää sovellusta eri tavoin kuin mitä sovelluksen määrittelyssä ja suunnittelussa on tarkoitettu, tällöin sovellus voi toimia virheellisesti ja antaa käyttäjälle mahdollisuuden hyödyntää sovelluksessa olevia virheitä aiheuttaen pahimmillaan vahinkoa liiketoiminnalle. Sovellusten riskienhallinnalla pyritään löytämään nämä kriittiset pisteet ja rajoittamaan virheellisten toimintojen käyttömahdollisuutta.



OWASP:n mukaan: *What Are Application Security Risks? Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention.*

Sovelluksen riskeistä on pyritty tunnistamaan yleisemmin esiintyvät vahingolliset virheet. tällöin usein viitataan ns. OWASP Top 10 -listaan. Sovellusten Top 10 haavoittuvuuksista on suomenkielinen versio, mutta se ei ole aivan ajan tasalla vuosittain päivittyvän englanninkielisen version rinnalla. (OWASP Top 10)

Sovellusten tietoturvariskeistä on yleisemmin käytetty termiä sovelluksen haavoittuvuus. (OWASP): *Although previous versions of the OWASP Top 10 focused on identifying the most common "vulnerabilities", they were also designed around risk. The names of the risks in the Top 10 stem from the type of attack, the type of weakness, or the type of impact they cause. We chose the name that is best known and will achieve the highest level of awareness.*

3.3 Käyttötapaukset

Käyttötapaus kertoo, mitä reaalimaailmassa tapahtuu, käyttötapaus kuvaa yrityksen tarjoamia palveluita, liiketoimintaprosesseja ja tehtäväketjuja. Käyttötapauksen avulla sovellusten suunnittelussa pyritään kertomaan mitä sovelluksen pitäisi tehdä.

3.4 Väärinkäyttötapaukset

Väärinkäyttötapaus kertoo mitä reaalimaailmassa voi tapahtua, väärinkäyttötapaus kuvaa miten palveluita, liiketoimintaprosesseja ja tehtäväketjuja voidaan yrittää käyttää väärin, niin että määrittelyssä, suunnittelussa toteutuksessa tunnistamattomien riskien avulla voidaan aiheuttaa vahinkoa palvelulle.

3.5 Haavoittuvuus

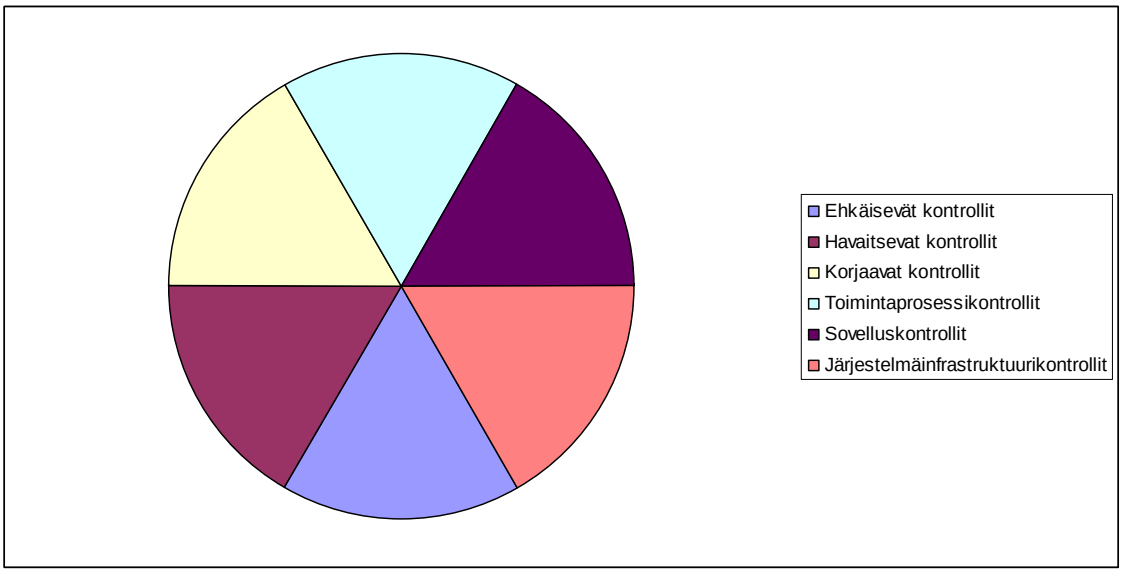
Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Esimerkiksi ohjelmistossa voi olla haavoittuvuus, joka mahdollistaa järjestelmän väärinkäytön. (TEPA)
Haavoittuvuus, tietoturvariski (OWASP), myöhemmin riski.

3.6 Tietoturvakontrolli

Tietoturvakontrolleilla tarkoitetaan sovellukseen/palveluprosessiin määriteltyjä ja rakennettuja tarkistuspisteitä joilla havaitaan virheet, virheellinen käsittely, tietoturvatapahtumat.

Tietoturvakontrolleilla luodaan mahdollisuudet toiminnan seuraamiseen ja kehittämiseen sekä sovelluksen ja palveluprosessien laadun parantamiseen.

Tutkielmaan kerättyjä tietoturvakontrollityyppejä, luettelo ei ole täydellinen, mutta kontrolliluettelo on suuntaa-antava, minkä tyyppisiä kontrollirakenteet voivat olla.



Havainnekuva tietoturvakontrolleista, tutkielma ei ota kantaa eri kontrollityyppien painoarvoon tai jakaumaa, kuvassa jokaiselle kontrollityypillä yhtäsuuri jakauma.

Kontrollityyppejä

- Ehkäisevät kontrollit
    - pääsykontrollit
        - käyttäjän tunnistaminen
        - käyttäjätunnus – salasana
        - käyttöoikeuksien hallinta
        - käyttöistunnon hallinta
    - syöttökontrollit
        - syötteiden sisällön tarkistukset
        - syötteiden pituuden tarkistukset
    - tulostuskontrollit
        - virhekäsittelyt

- Havaitsevat kontrollit
    - tapahtumalokitiedostot
        - kontrollipisteiden määrittely

- käytönvalvonta raportit
    - kontrollipisteiden määrittely
- virheraportit
    - kontrollipisteiden määrittely
- tulostuskontrollit
    - tulosteet
    - virheilmoitukset

- Korjaavat kontrollit
    - varmuuskopiot
        - kopiointi järjestelyt
        - kopioiden säilytykset
        - kopioiden suojaukset
    - toipumissuunnitelmat
        - sovellusvirheistä toipuminen
        - virheellisen käytöstä toipuminen
        - teknisen ympäristön virheistä toipuminen
    - jatkuvuussuunnitelmat
        - järjestelmä luokittelu
        - suunnitelmat mahdollisesta rajoitetusta käytöstä
- Toimintaprosessikontrollit
    - muutostenhallinta
        - ylläpito
        - pienkehitys

- Sovelluskontrollit
    - automatisoidut sovelluskontrollit
        - sovellusohjelmaan koodatut ja tietokantoihin tallennetut käsittelyprosessit
            - raja-arvot
            - hälytysrajat

- liipaisimet (triggerit)

- manuaaliset sovelluskontrollit
  - toimintaprosessit
    - ohjeet
    - työrutiinit
    - työtehtävien eriyttäminen
      - ristiin tarkistukset
    - hyväksymismenettelyt
      - työnkulun ohjaus
      - raja-arvot
    - tiedon käsittely
      - kerääminen
      - luokittelu
      - jakelu
      - arkistointi
      - tuhoaminen

- Järjestelmäinfrastruktuurikontrollit
  - automatisoidut järjestelmäinfrastruktuurikontrollit
    - automatisoitu haittaohjelmien tunnistaminen
    - automatisoidut järjestelmien päivitykset
  - manuaaliset järjestelmäinfrastruktuurikontrollit

3.5 Vaatimusmäärittely

Vaatimustenmukaisuus - Tietoturvavaatimukset

Luottamuksellisuus - luottamuksellisuusvaatimukset

Eheys - eheysvaatimukset

Käytettävyys – jatkuvuusvaatimukset

Lainsäädännönvaatimukset

Sovellettava lainsäädäntö tulee tunnistaa ja niistä eriytyvät vaatimukset tulee dokumentoida, esimerkiksi henkilö-, terveystietojen, yksityisyydensuojan, vakuutus ja pankkisalaisuuden osalta.

Liiketoiminnan vaatimukset

Liiketoiminnan luottamuksellisuuden, häiriöttömyyden ja käytettävyyden, toiminnan seurattavuuden vaatimukset tulee tunnistaa ja dokumentoida.

Teknisen infrastruktuurin vaatimukset

Teknisen infrastruktuurin määrittelyt ja ennalta sovitut toimintatavat asettavat vaatimuksia toteutukselle ja toiminnallisuuksille.

Vaatimusmäärittelyä käytetään apuna riskien tunnistamisessa.

4. Riskienhallinta

On olemassa useita tietoturvastandardeja, joiden avulla organisaatiot voivat kehittää tietoturvallisuuttaan ja arvioida omien järjestelmiensä toimivuutta, käytössä olevat tietoturvastandardit eivät kuitenkaan suoranaisesti anna vastausta sovellustason riskienhallinnalle.

Yleisesti hyväksyttynä käytössä olevana tietoturvaohjeistuksena voidaan pitää Valtionvarainministeriön ohjauksessa syntynyttä V A H T I –ohjeistoa (www.vm.fi/vahti).

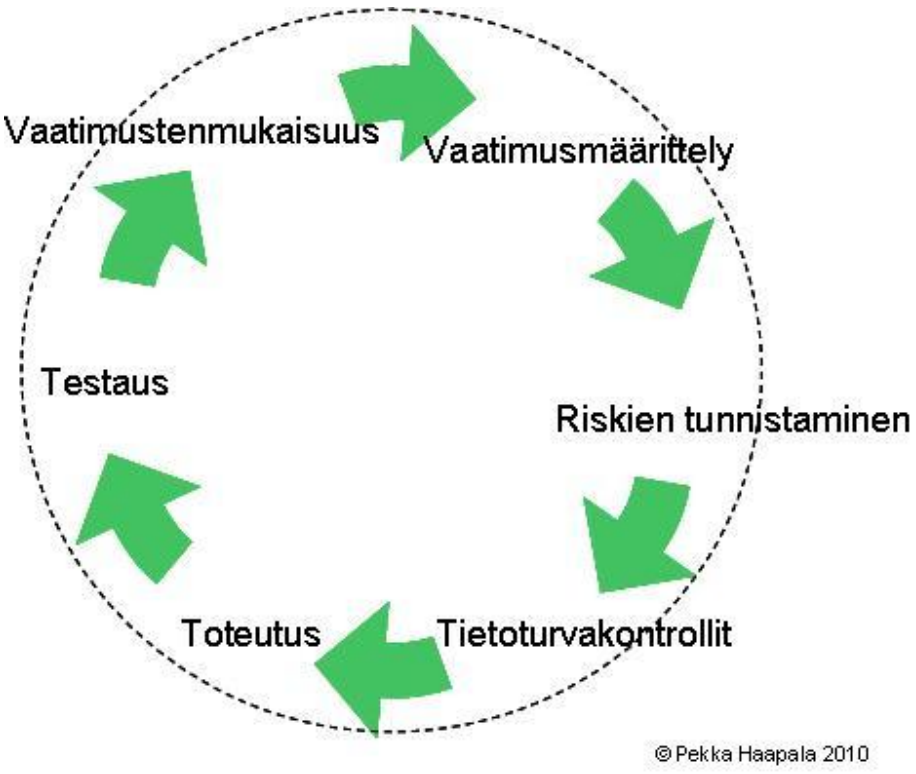
Tietojärjestelmän kehityksessä tulee pyrkiä siihen, että lopputuotteena oleva tietojärjestelmä vastaa niitä vaatimuksia, joita asetetaan kyseisen tehtävän hoidossa tietojen eheydelle, luottamuksellisuudelle ja käytettävyydelle. Järjestelmäkehityksessä riskien arviointi on tärkeää kaikissa vaiheissa. Esitutkimusvaiheessa riskianalyysin ja

alustavien tietoturvallisuusvaatimusten avulla arvioidaan vaadittavien tietoturvallisuuteen liittyvien toimintojen kustannus-, hyöty- sekä kuormitusvaatimukset, joiden pohjalta määritetään tärkeimmät tietoturvallisuusvaatimukset. Määrittelyvaiheessa tarkennetaan tietoturvavaatimukset. Tässä vaiheessa riskianalyysi toistetaan tarkemmalla tasolla. Riskianalyysin lisäksi tässä vaiheessa tuloksena on yleinen kuvaus jäännösriskistä sekä arvio tietoturvakriittisten kohteiden jäännösriskeistä. (Vahti, Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, 7/2003)

Riskienhallinta tulee ensisijaisesti perustua vaatimusmäärittelylle, vaatimusmäärittelyssä tunnistetaan:

- Tietoturvavaatimukset
- Lainsäädännönvaatimukset
- Liiketoiminnan vaatimukset
- Teknisen infrastruktuurin vaatimukset

Vaatimusmäärittelyä käytetään apuna riskien tunnistamisessa.



Riskien tunnistaminen niiltä osin mitä rakennettava sovellus tai määriteltävä prosessi aiheuttaa liitetoiminnan vaatimustenmukaisuudelle. Riskien tunnistaminen toimiin perustana kun määritellään ja rakennetaan sovellusten ja palveluiden tietoturvaa.

Tunnistettujen riskien perusteella pystytään määrittelemään kontrollipisteitä, tietoturvakontrolleja. Tietoturvakontrollien avulla rakennetaan toteutettavaan palveluun mekanismeja joilla riski havainnoidaan tai toteutetaan mekanismeja jotka estää riskin toteutumisen.

Riskien tunnistamisen myötä pystytään määrittelemään väärinkäyttötapaukset joiden tunnistaminen yhdessä tietoturvakontrollien kanssa luo pohjan ns. tietoturvatestaamiselle. Tietoturvatestaus termiä ei tulisi käyttää vaan tietoturva ominaisuuksien testaus on osa palvelun toiminnan ja laadun testaamista.

Riskien tunnistaminen jatkuu sovelluksen tai palvelun koko elinkaaren ajan, vaatimusten ja ympäristön muuttuessa.

5. Auditoinnit

Auditoinneilla tässä yhteydessä tarkoitetaan käyttöön otettavaan palveluun tehtävää testausta, joilla pyritään sovelluksen tai palvelun määrittelyssä, suunnittelussa, toteutuksessa havaitsematta jääneet tietoturvariskit. Pohjana riskien määrittelylle OWASP Top 10 riskit.

Ensivaiheessa tietoturva-auditoinnista saatu hyöty on löydettävissä sovelluksen/palvelun riskikartoituksessa määriteltyjen riskien pienentymisenä tai poistumisena kokonaan sekä uusien määrittelemättömien riskien todentamisena ja riskien poistamisena.

5.1 Yleisiä Tietoturva-auditoinnilla saatavia hyötyjä

Auditoinnilla pystytään turvaamaan toimintaympäristön vihamieleiseltä käytöltä löytämällä sovelluksen riskit ennen kuin joku ulkopuolinen hyödyntää niitä.

Auditoinnilla ja sen myötä tehtävillä korjauksilla pystytään välttämään riskien myöhemmän ilmitulon aiheuttama negatiivisen julkisuuden ja mahdollisen asiakkaiden luottamuksen menettäminen palveluun.

Auditoinnilla saadaan todennettua ja dokumentoitua sovelluksen riskit, sekä korjauksilla minimoitua tai poistettua kokonaan riskin vaikutukset.

Auditoinnin tuloksena pystytään estämään sovellusten/palvelun väärinkäytön sekä Havaitsemaan prosesseissa ja toimintamalleissa mahdollisesti olevat turvallisuutta heikentävät elementit. Kaiken kaikkiaan auditoinneilla pystytään määrittelemään ja todentamaan sovelluksen / palvelun sen hetkinen turvallisuustaso.

Auditointien avulla pystytään todentamaan lainsäädännön ja esimerkiksi valvovien viranomaisten edellytykset.

5.2 Tietoturva-auditoinnin aiheuttamia riskejä

Mikäli auditointi toteutetaan jo tuotannossa olevaan verkkopalveluun, niin mahdollisena auditoinnin aiheuttamana riskinä on palvelun kaatuminen. Riskin toteutuminen tarkoittaisi sitä, että sama asia voi toteutua kenen tahansa asiakkaan palvelun käytön seurauksena, jolloin tämän riskin toteutumisen vaikutukset ovat huomattavasti suuremmat.

Riskin aiheuttava toiminnallisuuden puute ja sen löytyminen auditoinnin myötä hallitusti on korjattavissa huomattavasti nopeammin.

Auditointiriskinä voidaan pitää myös mahdollista lokitiedostojen ja levyjen täyttymistä. Riski pystytään minimoimaan etukäteen tehtävillä tarkistuksilla ja toimenpiteillä.

5.3 Auditointien tuloksia

Yrityksessämme on vuodesta 2006 suoritettu säännöllisesti tietoturva-auditointeja, pääsääntöisesti tuotantokäyttöön otettaviin palveluihin, ennen tuotantokäytön alkua. Auditointien tavoitteena löytää sovelluksissa olevat riskit ja korjata riskien aiheuttajat ennen tuotantokäytön aloittamista.

Taulukko 1 kuvaa karkeasti löydettyjä riskejä. Vuositasolla löydettyjen riskien lukumäärää ei voi vertailla, koska luvuissa ei ole huomioitu auditointien lukumäärää vuodessa. Taulukosta voi huomioida lähinnä löydettyjen riskien riskitason merkittävyyden sekä erityyppisten riskien jakauman vuosittain ja riskien muutoksen. Riskien muutoksena tai kehityksenä voidaan pitää tietämystä riskeistä ja niiden hyväksikäyttötapojen kehittymisenä.

Taulukossa 2. Suomennetut riskikuvaukset vuodelta 2007
http://www.owasp.orgindex.php/Top_10_2007_Finnish

Ajantasaiset riskikuvaukset, *http://www.owasp.org/index.php/Top_10_2010-Main*

Taulukko 1.

	2006	2007	2008	2009	2010
Total Vulnerabilities	48	8	50	14	48
Level 5	0	0	0	3	0
Level 4	9	2	0	0	1
Level 3	0	4	50	4	19
Level 2	39	2	0	7	26
Level 1	0	0	0	0	2
SQL Injection		2			
Unverified Input	0	0			
Forceful Browsing		0			
Session Management	0	0			
Parameter Tampering		6	0		
Poor Error Handling	9	0			
Insecure Storage	0	0	0		
Denial of Service (DoS)	0	0			
Poor Configuration Management	0	0			
Information Gathering	0	0			
Buffer Overflows	0	0			1
Broken authentication and session management	0	0		0	1
Cross Site Scripting (XSS)	30	0	50	3	17
Injection Flaws	9	0	0	0	1
Malicious File Execution			0	0	0
Cross Site Request Forgery			0	0	1
Information Leakage and Improper Error Handling			0	1	7
Insecure Cryptographic Storage			0	0	0
Insecure Communications			0	0	0
Failure to Restrict URL Access			0	2	1
Insecure direct object reference				7	7
Insuffisient transport layer protection					0
Unvalidated redirects and forwards					0
Other				1	7

6. Johtopäätökset

Verkkosovellusten tietoturvan huomioiminen pitää osata huomioida jo vaatimusmäärittelyssä kun uuden palvelun rakentamista aloitetaan määrittelemään.

Vaatimusmäärittely luo pohjan riskien tunnistamiselle, on pyrittävä löytämään riskit jotka voivat estää tai haitata vaatimusten toteutumista. Riskien määrittely nähdään monesti liian hankala tai liian isona asiana, jota ei osata suhteuttaa olemassa olevaan ongelmaan. Riskien määrittely yksinkertaisimmillaan vastaa kysymykseen mikä tässä asiassa voi mennä pieleen.

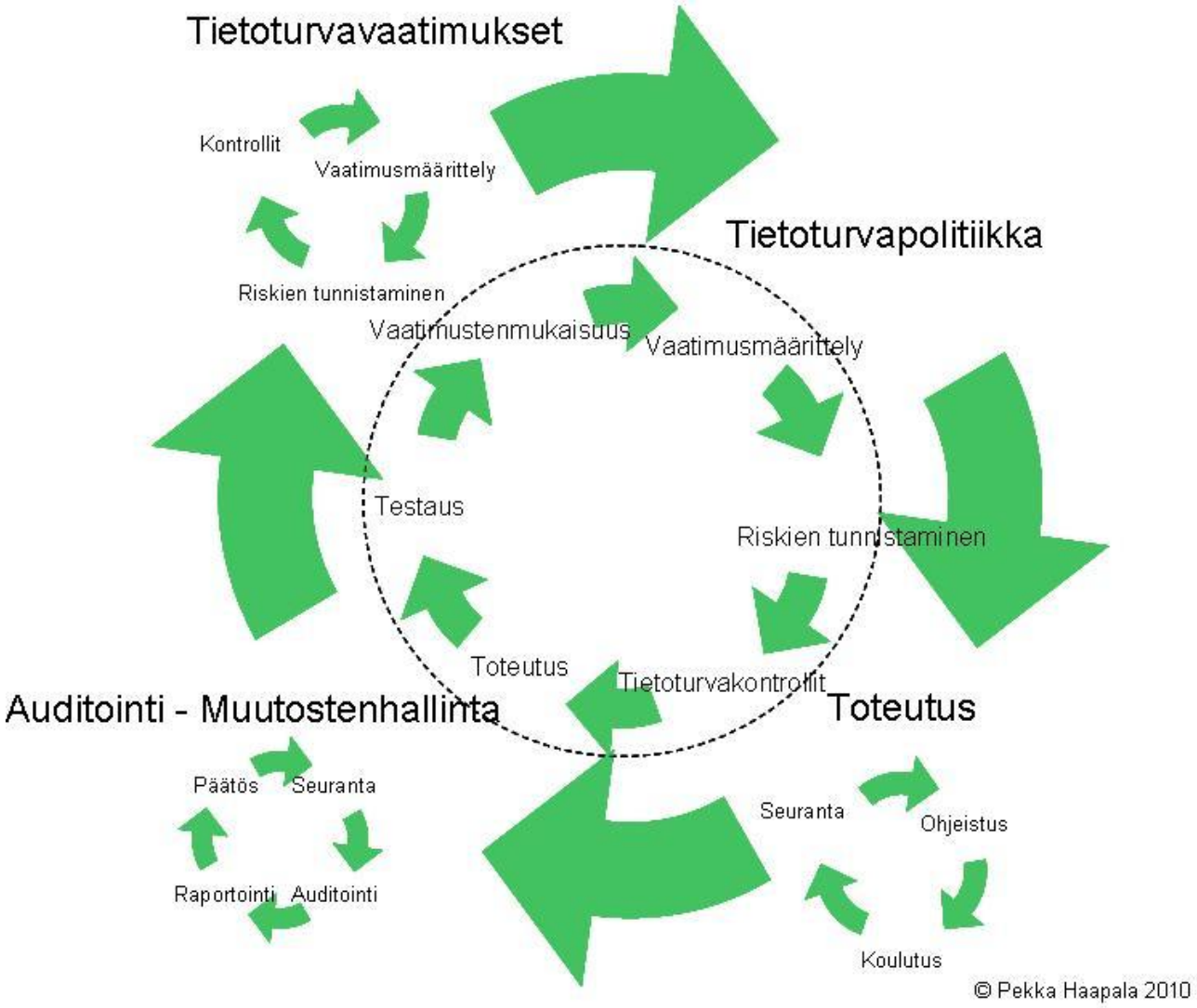
Verkkosovellusten käyttöä määriteltäessä määritellään käyttötapauksia kuvaamaan palvelun normaalia käyttöä, tässä riskienhallinnan näkökulmasta on myös varmasti helppo ajatella että miten käytän tätä palvelua väärin. Näiden väärinkäyttötapausten määrittely edelleen edesauttaa löytämään riskejä, asioita jotka voi mennä pieleen.

Kun riskien tunnistaminen on saatu tehtyä, pystytään määrittelemään kontrollipisteitä, kontrollimekanismeja – tietoturvakontrolleja joilla pyritään havaitsemaan onko aikaisemmin määritelty riski toteutumassa. Kappaleessa 3.4 on kuvattu sovelluskontrolleja, sovellukseen sisään rakennettavia mekanismeja joilla riskiä pystytään hallitsemaan. Yhtä tärkeitä kuin sovelluskontrollit, ovat havaitsevat kontrollit, joiden avulla kirjoitetaan esimerkiksi tapahtumatiedostoon lokitietoa palvelun käytöstä, tai vaihtoehtoisesti lähetetään hälytys väärinkäyttötapauksesta.

Riskien tunnistaminen, siitä johdetut tietoturvakontrollit ovat myös pohjana tietoturvarakenteiden testaamiselle, termiä tietoturvatestaus ei pitäisi käyttää, koska sovelluksentestauksen yhtenä osana on testata aikaisemmin määriteltyjä kontrollirakenteita, miten tarkistuspisteet toimivat ja havaitsevat. Mikäli näiden kontrollipisteiden määrittely ja toteutus jää tekemättä, niin sovellustestaus vaiheessa on mahdoton löytää vastausta kysymykseen: ”Miten teen sovellukselle tietoturvatestausta?”

Testaus jakson jälkeen pystytään todentamaan, vastaako sovellus määriteltyjä vaatimuksia, toteutuuko vaatimusten mukaisuus?

Riskien tunnistamisen puutteellisuuden syinä voidaaan löytää sovelluskehittäjien puutteellisen riskienhallinta osaamisen, suurinpana syynä kuitenkin voidaan pitää määrittelyvaiheessa tehtävän riskientunnistaminen epäonnistumisen.



Puutteellisen riskienhallinnan korjaaminen sovelluksen myöhemmässä toteutuksessa voi olla hankalaa ja huomattavasti kalliimpaa kuin, että riskienhallinta ja sitä kautta tietoturvan toteuttaminen olisi tehty oikea-aikaisesti.

Sovelluksen testauksen jatkona kannattaa harkita erillisen tietoturva-auditoinnin

toteuttamista, jolla pyritään löytämään riskejä joihin ei ole osattu varautua.
Auditointi ei saa jäädä kertaluotoiseksi tapahtumaksi jota toteutetaan esimerkiksi vain tuotanto käyttöönoton yhteydessä, vaan auditointi, aivan kuten riskienhallinta tulee nähdä sovelluksen elinkaaren mittaisena prosessina joka tulee aika-ajoin toteuttaa uudestaan.

Sovelluksen tietoturvan varmistamisessa yhtenä elementtinä on käytettävään kehitysympäristöön rakennettavat, tunnettuihin riskeihin liittyvät kontrollit, framework:t joilla pyritään rajaamaan mahdollisuudet toteuttaa sovelluspalvelua niin, että siinä ko. riskit voisivat toteutua. Tämän käsittely on rajattu ulkopuolelle.

Yleisenä johtopäätöksen tai huomiona voisi todeta, kuten johdannossa on OWASP Helsingin kommentoimana. Painopiste yleisesti Tietoturvapanostuksissa on teknisen ympäristön kehittämisessä, verkkosovelluksiin liittyvät riskit jäävät usein huomioimatta ja tunnistamatta..

Lähteet:

Keskusrikospoliisi, rikostietopalvelu, 7.10.2009, Arkistoviite KRP/RTP 5230/213/09)

www.nixu.com/blogi/2010/huhtikuu/uudessa-owasp-top-10ssa-injektiot-jyllaavat/

www.owasp.org/index.php/File:2010-T10-ArchitectureDiagram.png

www.owasp.org/index.php/Top_10_2007_Finnish

(OWASP Top 10)

http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf

(TEPA) Sanastokeskus, TSK 31, Tiivis Tietoturvasanasto

(OWASP) www.owasp.org/index.php/Top_10_2010-Main

(Vahti) (http://www.vm.fi/vahti)

Vahti, Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, 7/2003