

*Tässä Relator Oy:n tuottamassa White Paper -julkaisussa käsitellään sovellusten hankkimista sekä sovelluskehitystä tietoturvan näkökulmasta. White Paperin ovat kirjoittanut Relator Oy:n konsultit Kimmo Kaario, Riku Nykänen ja Juha Pakkanen.*

## Tietoturvan huomioon ottaminen tietojärjestelmähankinnassa

Sovellusten tietoturva ei ole pelkästään tietoturvan huomioon ottamista toteutuksessa ja teknologiavalinnoissa, vaan se on laajempi kokonaisuus alkaen kohdeorganisaation kokonaisarkkitehtuurista ja päättyen järjestelmän poistoon käytöstä. Pelkät teknologiavalinnat eivät takaa sovelluksen tietoturvallisuutta, vaan tietoturva on kokonaisuus, jossa tulee ottaa huomioon myös prosessit, tiedonhallinta, käyttäjät, laitteet, käyttöympäristö ja muut resurssit. Turvallisuuden takaamiseksi sovelluksen käyttöön liittyvien prosessien ja muun toimintaympäristön tulee olla kunnossa, vaikka sovellus olisikin toteutettu käyttäen parhaita menetelmiä.

### Mitä on tietoturva?

Perinteisessä määritelmässä tietoturvallisuus koostuu kolmesta osatekijästä, jotka ovat

- luottamuksellisuus
- käytettävyys
- eheys

Näistä korostetaan usein luottamuksellisuutta, jolla tarkoitetaan sitä, että tieto on vain tietosisältöön oikeutettujen henkilöiden käytettävissä. Käytettävyydellä tarkoitetaan tiedon saatavuutta oikeassa muodossa oikeaan aikaan ja eheydellä tiedon rakenteellista oikeellisuutta.

Laajennetuissa määritelmissä on yleensä mukana edellisten lisäksi

- kiistämättömyys
- tunnistaminen (todentaminen)

Kiistämättömyydellä tarkoitetaan kykyä todistaa tapahtumat tapahtuneeksi myöhemmin siten, ettei toinen osapuoli voi kiistää tapahtunutta.

Todentaminen (autentikointi) tarkoittaa osapuolten (henkilöt, järjestelmät tai muut entiteetit) tunnistamista.

Kun kaikelle tietojärjestelmän sisältämälle tiedolle ja toiminnoille toteutuvat edellä mainitut viisi osatekijää, voidaan järjestelmää pitää tietoturvallisena. Valitettavasti esitettyjä vaatimuksia on vaativaa testata, joten yksikäsitteisen vastauksen antaminen järjestelmän turvallisuudesta on käytännössä mahdotonta.

Määritelmä ei yksin anna konkreettisia työvälineitä tietoturvallisen toimintaympäristön rakentamiseen ja kehittämiseen. Määritelmästä on kuitenkin apua siinä vaiheessa, kun tietoturvallisuuden tarve on tiedostettu ja kaikkea tekemistä pystytään peilaamaan määritelmää vasten. Tämä tarkoittaa sitä, että esimerkiksi prosesseja kehittäessä, järjestelmävaatimuksia määriteltäessä ja sovelluskoodia kirjoitettaessa tuotoksia testataan määritelmän osatekijöitä vastaan.

## Tiedon arvon määrittely

Lähes kaikki tietoturva-asiantuntijat ovat yksimielisiä siitä, että tietoturvallisesti 100% varmaa ympäristöä ei ole. Käyttämällä enemmän resursseja on kuitenkin mahdollista parantaa tietoturvaa. Tietoturvan parantaminen pitää sisällään useita asioita kuten

- tehdä tiedon väärinkäyttö mahdollisimman hitaaksi ja hankalaksi, jolloin väärinkäytön havaitsemisen todennäköisyys kasvaa.
- minimoida vahingot poikkeaman tapahtuessa.
- minimoida resurssit, jotka tarvitaan poikkeamasta palautumiseen.

Tämän vuoksi olennainen osa sopivan tietoturvatason saavuttamista on tuntea, minkä arvoista käytettävissä oleva tieto on. Kun tiedon arvo tunnetaan, pystytään se huomioimaan liiketoimintaprosesseissa sekä sovelluksen arkkitehtuurissa ja teknologiavalinnoissa. Näin resurssit voidaan kohdistaa liiketoiminnan jatkuvuuden kannalta optimaalisella tavalla.

Organisaation sisältä tulevien hyökkäyksien osuus kaikista hyökkäyksistä vaihtelee tutkimusten mukaan 20 prosentista yli 50 prosenttiin. Näitä hyökkäyksiä voidaan ehkäistä rajoittamalla pääsyä kriittiseen tietoon liiketoimintaprosesseissa. Yksi helpoimpia tapoja parantaa tietoturvaa on yksinkertaistaa liiketoimintaprosesseja. Kun tietoa sisältäviä järjestelmiä ja niiden käyttäjiä on vähän, on myös tietoturvariskejä lähtökohtaisesti vähemmän. Tämä on kuitenkin harvoin mahdollista, mutta uusia järjestelmiä hankittaessa samanaikainen liiketoimintaprosessien muuttaminen voi saada aikaan merkittäviä parannuksia tietoturvaan.

Jokainen yksittäinen käyttäjä, jolla on pääsy liiketoimintakriittiseen tietoon tai sitä sisältävään tietojärjestelmään, muodostaa mahdollisen

tietoturvariskin. Sen vuoksi tiedon saatavuuden rajaaminen mahdollisimman pienelle käyttäjäjoukkoille sekä yksittäisiin järjestelmiin parantaa tietoturvaa. Luonnollisesti jossain kohti kulkee raja, jolloin tiedon saatavuuden rajoittaminen haittaa enemmän organisaation toimintaa kuin parantaa tietoturvaa. Sen vuoksi tavoitteena onkin löytää paras mahdollinen tietoturvallinen ratkaisu liiketoiminnan ehdoilla.

## Vaatimuksilla parempaa tietoturvaa

Jokaisen tietojärjestelmähankinnan perusta pitäisi olla vaatimusmäärittely, joka määrittelee kaikki järjestelmälle kuuluvat vaatimukset. Vaatimusmäärittely tulee tehdä aina riippumatta siitä, onko hankittava järjestelmä valmisohjelmisto vai räätälöity järjestelmä. Vaatimusmäärittelyn osana määritellään myös kaikki järjestelmän tietoturva-vaatimukset.

Tietoturva-vaatimuksia on hyvin monen tyyppisiä, kuten esimerkiksi:

- käyttäjän tunnistus ja oikeuksien hallinta
- tapahtumien jäljitettävyyttä
- tietojen salaaminen
- varmuuskopiointi ja palautuminen

Yksittäiseen järjestelmään on helppo määritellä satoja tietoturvaan liittyviä vaatimuksia. Hyvin usein sekä toiminnalliset että ei-toiminnalliset tietoturvaan liittyvät vaatimukset voidaan kirjoittaa yleiskäyttöiseen muotoon, jolloin niitä voidaan käyttää tehokkaasti uudelleen. Sama pätee myös vaatimuksia vastaan tehtyihin testitapauksiin. Käyttämällä myös muodostunutta referenssivaatimustietokantaa voidaan varmistua, että kaikki olennaiset tietoturva-vaatimukset tulevat huomioiduksi.

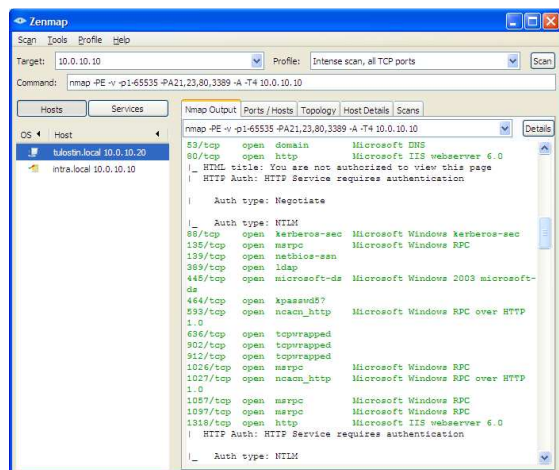
## Tietoturva sovelluskehityksessä

Suurin osa ohjelmistojen haavoittuvuuksista johtuu ohjelmointivirheistä, kuten puskureiden ylivuodoista. Nämä virheet voidaan usein havaita

automaattisilla koodin analysointiohjelmistoilla, jotka on kehitetty testauksen automatisoinnin näkökulmasta. Vaikka näitä ohjelmistoja on myös vapaasti saatavilla, niitä käytetään todella vähän tietoturvan parantamisen näkökulmasta.

Koska web-sovellukset ovat erityisen alltiita hyökkäyksille, niiden tietoturvatestaukseen on kehitetty sekä menetelmiä että sovelluksia. Yksi merkittävimmistä hankkeista on The Open Web Application Security Project (OWASP). OWASP on avoin yhteisö, jonka tavoitteena on kehittää menetelmiä web-sovellusten tietoturvan parantamiseen. OWASP ei keskity pelkästään kehittämään yhtä tietoturvan osa-aluetta, vaan sisältää useita aliprojekteja. Nämä kehittävät muun muassa ohjeita, viitekehyksiä ja sovelluskomponentteja.

Haavoittuvuusanalyysin avulla voidaan selvittää yksittäisen järjestelmän turvallisuuden taso. Tällöin analysissä käytetään valittua joukkoa automaattisia analysointityövälineitä sekä manuaalisesti suoritettavia testejä.



**Kuva: NMAP turvallisuusskanneri**

Usein käytettävät työvälineet ovat samoja, joita käytetään oikeissa hyökkäyksissäkin. Suurin osa ohjelmistoista on lisäksi vapaasti käytettävissä, joten testaus vaatii pääasiassa vain osaamista ja aikaa. Testisuunnitelma on usein sellaisenaan

uudelleenkäytettävissä, jolloin pyörää ei tarvitse joka kerta keksiä uudestaan. Hyvä testisuunnitelma takaa sen, että testaus on riittävän kattavaa.

## Avoimen lähdekoodin tietoturva

Usein kuulee väitteitä, että avoimen lähdekoodin ohjelmistot ja komponentit eivät olisi turvallisia. Vastaava väite voidaan osoittaa myös kaupallisille, suljetun koodin ohjelmistoille. Molemmat joukot ovat niin heterogeenisiä, että kummastakin löytyy sekä turvallisia että riskialttiita sovelluksia.

Avoimen lähdekoodin sovellukset tarjoavat käyttäjälleen mahdollisuuden analysoida sovelluksen tietoturvaa kooditasolla, kun taas suljetun koodin sovelluksissa joudutaan luottamaan toimittajaan. Lisäksi useissa tutkimuksissa on havaittu, että aktiiviset avoimen lähdekoodin yhteisöt tuottavat ratkaisun raportoituihin ongelmiin nopeammin kuin kaupalliset yritykset.

Asiantuntijat ovat myös selvittäneet, että avoimen lähdekoodin sovelluksiin tahallisesti tai tahattomasti sisältyvät haavoittuvuudet löytyvät nopeammin kuin suljetun lähdekoodin sovelluksista. Tämä johtuu siitä, että varsinkin aktiivisissa avoimen lähdekoodin projekteissa useat henkilöt seuraavat aktiivisesti kaikkia projektissa tehtyjä koodimuutoksia.

## Valvontajärjestelmä osana kokonaisarkkitehtuuria

Tietojärjestelmiä kehittävät organisaatiot rajaavat usein oman vastuunsa tuotteen tietoturvasta kehitysprojektin aikaiseksi. Hyvin harvat tuotteet pitävät sisällään ominaisuuksia, joilla voidaan valvoa tuotteisiin kohdistuvia hyökkäyksiä käytön aikana.

Räätälöityjen järjestelmien osalta tulisi ottaa huomioon tuotantoympäristön valvontajärjestelmät jo vaatimusmäärittelyvaiheessa. Kun järjestelmiin

sisäänrakennetaan integraatio valvontajärjestelmiin, niin valvontajärjestelmä voi tarjota näkymän yrityksen tietoturvan tilannekuvaan.

Valvontajärjestelmien ei tarvitse välttämättä olla kalliita, vaan useimpien PK-yritysten valvonta pystytään toteuttamaan kustannustehokkaasti avoimen lähdekoodin sovelluksilla. Yksi esimerkki tällaisesta sovelluksesta on Nagios. Se tukee valmiiden lisäosien kautta esimerkiksi verkkolaitteiden, palvelinten komponenttien, levytilan ja tietokantojen valvomista. Lisäksi Nagios tarjoaa rajapinnan, jonka avulla voidaan valvoa yrityksen räätälöityjä järjestelmiä. Valvonnan kautta on mahdollista havaita tietoturvarikkeitä mahdollisimman aikaisin ja pyrkiä minimoimaan vahingot, jopa automaattisesti. Tämä luonnollisesti edellyttää, että tähän on varauduttu jo järjestelmän määrittelyvaiheessa ja erityisesti järjestelmän tietoturvaan liittyvissä vaatimuksissa.

Toinen valvonnan muoto ovat tunkeutumisen tunnistusjärjestelmät (Intrusion Detection System, IDS). Nämä järjestelmät pyrkivät havaitsemaan verkkoliikenteestä tai muusta tietolähteestä tunkeutumisyrityksiä. Useimmat IDS-järjestelmistä perustuvat tunnistäjälkiin eli ennalta havaittuihin malleihin hyökkäyksissä. Tämä tekeekin IDS-järjestelmät haavoittuviksi uudentyypisiä hyökkäyksiä kohtaan, joten paraskaan IDS-järjestelmä ei tarjoa 100% suojaa.

## Tietoturva-auditoinnilla ongelmat esiin

Tietoturvan kehittäminen on jatkuva prosessi. Organisaation järjestelmien ja toiminnan kehittyessä toimintaympäristön muutos saa aikaan uusia haavoittuvuuksia. Lisäksi erilaiset hyökkäysmekanismit kehittyvät jatkuvasti. Säännöllisellä auditoinnilla pystytään havaitsemaan tietoturvan kehittämiskohteita ennen kuin haavoittuvuuksia ehditään hyväksikäyttää.

Tietoturva-auditoinnissa voidaan arvioida joko organisaation kokonaistietoturvan tilannekuva tai valittu osa siitä, esimerkiksi uusi tietojärjestelmä ja siihen liittyvät prosessit.

## Tietoarkkitehtuuri ja tietoturva

Riippuen organisaation tietoarkkitehtuurin sekä tiedon mallintamisen tasosta tietoturva on mahdollista ulottaa esimerkiksi dokumenttitasolta aina rakenteisen tiedon elementteihin saakka.

Yksi kiinnostavimmista tietoturvan kehittämiskohteista on monitasotietoturvan käyttöönotto organisaatiossa. Monitasotietoturvalla (Multilevel Security, MLS tai Content-based Information Security, CBIS) tarkoitetaan karkeasti ottaen oikeuksien määrittämistä siten, että henkilöllä on näkymä vain niihin tietoihin, joihin hänen oikeutensa riittävät. Tähän liittyy kiinteästi tiedon rakenteisuus – esimerkiksi yhdessä asiakirjassa voi olla useita eri käyttöoikeuksia sisältäviä rakenneosia.

Monitasotietoturva voi tarkoittaa käyttäjien näkökulmasta esimerkiksi, että laajemmat käyttöoikeudet omaava käyttäjä näkee dokumentin sisällöstä kaiken, kun rajallisemmat käyttöoikeudet omaava henkilö taas näkee esimerkiksi vain johdannon. Monitasotietoturva voi myös itse tietosisällön rajoittamisen lisäksi rajata tietoon kohdistuvia toimenpiteitä kuten tulostamista.

Kun tieto itsessään on jo suojattu sisäisesti roolien tai käyttäjäkohtaisten oikeuksien mukaisesti, ei tiedon väärinkäyttö onnistu niin helposti, koska tiedoston haltuun saaminen ei vielä tarkoita, että koko tiedoston sisältö on automaattisesti nähtävissä.

Monitasotietoturvan toteuttamiseenkin on jo tarjolla joitakin välineitä, kuten Microsoftin Rights Management Services (RMS) Windows Server-käyttöjärjestelmälle. Sen avulla voidaan toteuttaa yksinkertaisimpia monitasotietoturvan

