TTY / TIE / J. Koskinen

Ei laskimia. Kysymyspaperin saa pitää.

TIE-30500 Identiteetin- ja pääsynhallinta, IAM

Tentti (I) 6. 3. 2014

Arviointiin käytetään POPissa esitettyä kokeellista mallia, josta on muistutettu tentin edellä. Tiivistäen (arvosanat 2 ja 4 unohtaen): Kukin kelvollinen vastaus arvioidaan pisteillä eli tasoilla 1, 3 tai 5 sen mukaan, edustaako vastaus ymmärryksen, soveltamisen vai analyysin tasoista osaamista. Jos vastauksia puuttuu tai jos paras vastaus on tasolla 1, tentti hylätään. Jos paras vastaus on tasolla 3, arvosanaksi tulee '1'. Jos tason 5 vastauksia on ainakin yksi ja loput ovat vähintään tasolla 3, tulee arvosana '3', paitsi jos kaikki ovat tasolla 5, jolloin tulee arvosana '5'.

Vastaamisessa on siis tärkeää, että vastaa tasaisen hyvin kaikkiin tehtäviin eikä tyydy vain toistamaan tai edes selittämään asiaa niin kuin se on materiaalissa (= taso 1). Pistemäärä 5 ei edellytä täydellistä vastausta. Perinteinen arvosanan '5' raja on 25 pistettä, kun tehtävät arvioidaan 0–6 pisteeseen. Siihen verrattuna nyt tavoiteltavan tason 5 voi ajatella vastaavan perinteisen arvioinnin viittä pistettä kuudesta. Muuta yhtäläisyyttä ei paljon ole. Erityisesti tasoja ei summata arvosanan määrittämiseksi.

Tehtävien otsikot vastaavat POPissa esitettyä ydinaineksen jaottelua ja aiheissa ovat mukana kurssin kuluessa tehdyt lisäykset.

1. IAM-perusteet. Kirjoita jäsennelty esitys hakemiston ja sen teknisten ominaisuuksien merkityksestä identiteetinhallinnassa.

2. Autentikointi. Tarkastellaan IB-kryptoa eli identiteettipohjaista kryptoa tällä abstraktiotasolla: Julkisen avaimen kryptosysteemin avain on kenen tahansa johdettavissa yksilön tai laitteen identiteetistä, ja yksilö itse tai laite saa vastaavan yksityisen avaimen luotetulta palvelimelta mutta ei kukaan muu. Mitä yksilöiden tai laitteiden autentikointiin liittyviä tehtäviä voitaisiin ratkaista IB-kryptolla ja millä tavoin?

3. Käyttövaltuudet. Tee selkoa käsitteistä attribuutit, roolit, ryhmät ja hierarkiat sekä näiden yhteyksistä toisiinsa, kun tavoitteena on järjestää käyttövaltuuksien hallinta tehokkaasti. Oleta, että identifioinnin ja autentikoinnin haasteet on ratkaistu erikseen.

4. Organisaatio. Oletetaan, että organisaatiossa otetaan käyttöön keskitetty IAM yhdistämään aiemmin erillään toimineita järjestelmiä, mutta kaikkia järjestelmiä ei kytketä samalla kerralla ja joitakin jätetään kytkemättä. Mitkä ovat järkeviä perusteita tällaiselle vaiheistukselle, ja millä perusteilla kannattaa valita vaiheiden työkohteet ja erilleen jätettävät järjestelmät?

5. Federaatio. Henkilö H haluaa www-selaimensa kautta käyttää sovellusta A, jonka omistavalla yrityksellä Y ei ole tietoa hänestä eikä A:n käyttäminen Y:n palvelimella vaadi sitä. Henkilön H työpaikka T sopii Y:n kanssa siitä, että se maksaa Y:lle A:n käytöstä, kunhan Y toimittaa T:lle tiedot siitä, kuka A:ta on käyttänyt ja milloin. Organisaatiot T ja Y perustavat IAM-federaation yhdessä muiden vastaavien kanssa tai liittyvät jo olemassa olevaan, sillä A:n tarvetta esiintyy T:ssä paljon. Tuloksena on, että syöttämällä selaimeen nimensä ja salasanansa H pääsee käyttämään A:ta, ja uloskirjautumisen jälkeen (tai laskutuksen aikaan) T saa Y:ltä tiedon käytöstä. Selvitä, millaisten paikkojen ja prosessien kautta H:n nimi ja salasana sekä käyttöaika kulkevat T:n lokitietoihin. Tason 3 vastaukseen riittää selvittää tiedon kulku siihen vaiheeseen asti, että H saa A:n auki.