Käyttäjät kateissa, oikeudet omilla teillään!

Pekka Hankela
Helsingin kauppakorkeakoulu

Rakkaalla lapsella on monta nimeä: puhutaan käyttäjähallinnosta, pääsynhallinnasta, identiteetinhallinnasta, sähköisestä identiteetistä ja monesta muusta. Varsinkin englanniksi termejä löytyy tukuittain. Mikä tämä kummajainen on, ja miten se liittyy yliopistoon? Mihin sitä tarvitaan? Emmekö voisi vain käyttää sähköisiä palveluita?

Mikä ei ole palvelu, mutta silti palvelee?

Käyttäjähallinto on järjestelmä, jossa on sekä ihmisiä että tekniikkaa. Se on palvelu, jonka tehtävä on palvella muita palveluita. Palvelun palvelua on hyvin vaikea hahmottaa, koska sillä on hyvin vähän, jos ollenkaan, näkyviä osia. Oikeastaan se näkyy vasta, kun se ei toimi. Yksi esimerkki tästä on tilanne, jossa käyttäjä ei pääse käsiksi haluamiinsa kohteisiin, vaikkapa omaan sähköpostiinsa. Toimiessaan käyttäjähallinto sallii jouhevan tietojärjestelmien ja palveluiden hyödyntämisen.

Käyttäjähallinnon hyötyjä on vaikea mitata rahassa. Oikeastaan ainoa järkevä tapa on mitata sen haittoja tai mieluummin haittojen vähyyttä. Jos käyttää yhtä palvelua ja joutuu kirjautumaan sinne kerran, on kirjautumisesta melko vähän haittaa. Mutta mitä jos käyttää 20 palvelua ja kirjautuu 20 kertaa? Siitä on jo vaivaa käyttäjälle. Tässä vaiheessa nousee esiin hittisana ”kertakirjautuminen”. Sillähän voi välttyä turhilta kirjautumisilta, eikö? Kertakirjautumisessakin on riskinsä. Jos käyttäjän salasana ja tunnus joutuvat vääriin käsiin, väärinkäyttäjä pääsee samoilla oikeuksilla kaikkiin niihin 20 palveluun. Käyttöoikeuksia, kuten kananmunia, ei kannata eikä saa laittaa kaikkia samaan koriin.

Miksi siis panostaa käyttäjähallintoon? Keskitetyllä käyttäjähallinnolla tai ehkä mieluummin keskitetyllä näkymällä (käyttöliittymällä) hajallaan olevaan käyttäjätietoon voidaan hallita, ohjata ja tasapainottaa monen järjestelmän ja palvelun käyttöä. Käyttäjä pystyy hyötymään kertakirjautumisen ja muiden käyttöä helpottavien toimintojen eduista ilman, että hänen tarvitsee pelätä vääriin käsiin joutuneiden oikeuksien aiheuttavan vahinkoa. Tällöin oikeudet eri järjestelmiin ja palveluihin on myönnetty niin, ettei hukkuneista tai hakkeroiduista tunnuksista ole hallitsematonta riskiä. Toisaalta käyttöoikeuksien hallinnoija voi valvoa koko organisaation tunnusten käyttöä ilman, että hänen tarvitsee käydä läpi kaikki järjestelmät erikseen.

Yhtenäinen prosessi ja toimintamalli

Tekniikka ei ratkaise kaikkea, eikä varsinkaan käyttäjähallintoa. Toimiakseen kunnolla käyttäjähallinnon on noudatettava koko organisaatiossa yhtenäistä toimintamallia ja prosessia. On muutamia yksinkertaisia perusperiaatteita: käyttäjän tullessa organisaation jäseneksi hänen perustietonsa eli niin sanottu identiteettinsä luodaan vain yhteen paikkaan, josta se monistetaan muihin järjestelmiin. Kaikkien oikeuksien tulee perustua myönnettyyn lupaan, oli se sitten henkilön myöntämä tai organisaation toimintapolitiikkaan perustuva. Käyttöoikeuksien käyttöä tulee valvoa ja käyttäjän pitää olla tästä tietoinen. Oikeuksien tulee päättyä heti, kun käyttäjä ei enää ole organisaation jäsen tai perustetta niille ei enää ole.

Myyntipäällikkö **Riku Ahlroth** IBM Finland Oy:stä pitää tärkeänä, että yliopiston kaltaisessa organisaatiossa käyttäjähallinnon perusprosessit otetaan käyttöön keskeisissä järjestelmissä. Kun prosessit toimivat perustasolla, voidaan niitä helpommin laajentaa muihin järjestelmiin. Hänen

mukaansa yliopistoille erityisiä haasteita tuovat käyttäjien suuri vaihtuvuus ja hyvin heterogeeninen käyttäjäkunta.

Käyttäjähallinnon prosessi voidaan yksinkertaistaa jakamalla se viiteen päävaiheeseen: oikeuksien tarpeen syntyminen tai havaitseminen, hyväksyminen, oikeuksien myöntäminen, vahvistaminen ja oikeuksien käyttö. Viimeiseen vaiheeseen eli käyttöön liittyvät keskeisesti myös käytön seuranta ja raportointi.

<<Kuva 1>>

Rooleista edustuksiin

Toinen hittisana käyttäjähallinnossa on *roolit*. **Archie Reed** kuvaa kirjassaan *Definitive Guide to Identity Management*, kuinka rooleihin liitetyt oikeudet ratkaisevat useimmat organisaation käyttöoikeusongelmat. Rooleihin liitetään oikeuksia ja roolit liitetään käyttäjiin. Tällöin käyttäjä perii roolinsa mukaiset oikeudet. Muutettaessa roolin oikeuksia muuttuvat ne samalla käyttäjille.

Roolien käyttö varsinkin suuressa organisaatiossa on kuitenkin haastavaa. Roolit liitetään tyypillisesti tiettyyn toimeen tai asemaan organisaatiossa. Nämä voivat kuitenkin muuttua hyvinkin nopeasti ja siksi staattiset roolit eivät ratkaise ongelmaa. Erityisesti edestakaisin muuttuvat asemat ovat hankalia. Ongelma voidaan ratkaista käyttämällä edustuksia eli määrittelemällä, mitä tahoa käyttäjä kulloisessakin roolissaan edustaa.

Edustuksien moninaisuutta voi kuvata yliopistossa esimerkillä, jossa assistentti avustaa professoria tenttien korjaamisessa. Assistentti on koko ajan roolissa ”tentinkorjaaja”, mutta hänellä on monta edustusta. Jos hän kysyy etukäteen professorilta neuvoa, miten arvostella tentti yleensä, niin hän edustaa kaikkia opiskelijoita. Jos hän huomaa vaikeasti arvosteltavan tenttisuorituksen ja kysyy vasta sitten, miten arvostella, hänen tulee tehdä selväksi, edustaako hän opiskelijaa kysymällä juuri tietyn tenttisuorituksen arvostelua vai kaikkia tentin tehneitä kysymällä ohjetta yleisellä tasolla. Professorin vastaus riippuu siis sekä assistentin roolista korjaajana että edustettavasta tahosta – yksi opiskelija vs. kaikki tentin tehneet.

Sama roolien ja edustuksien ongelmanasettelu on myös yritysmaailmassa. Toimitusjohtaja **Olli Heikkilä** Panorama Partners Oy:sta kertoo, että käyttäjähallinto on selkeästi kehittymässä organisaatioiden välisen käyttäjähallinnon suuntaan. Roolit eivät enää riitä, eivätkä puumaiset käyttäjähakemistot toimi kompleksisessa ympäristössä. Hänen mukaansa edustusten käytöllä ja relaatiopohjaisilla käyttäjätietokannoilla pystytään vastaamaan tähän kehitystarpeeseen. Varsinkin pankki- ja vakuutusalalla on tilanteita, joissa yhdellä asianhoitajalla on lukuisia asiakkaita edustettavina. Esimerkiksi yksi vakuutusmeklari hoitaa usean asiakkaan vakuutuksia ja jokaista toimeksiantoa kohden hänellä voi olla eri oikeudet. Yhden nimissä hänellä on kymmenentuhannen euron rajoitus, kun toiselle hän saa tehdä 10 miljoonan transaktioita.

Käyttäjähallinto on monimuotoinen ja monimutkainen asiakokonaisuus. Asian tärkeyden ylenkatsominen, prosessien laiminlyönti, sekä roolien ja edustuksien unohtaminen johtavat herkästi kankeasti kehittyviin sähköisiin palveluihin. Sähköiset palvelut ovat käyttäjiä varten, joten käyttöä on myös hallittava.

Lähteet

Hankela, Pekka: Käyttäjähallintoprosessit – sovellus yliopistoon, Helsingin kauppakorkeakoulu 2005
Reed, Archie: Definitive Guide to Identity Management, realtimepublishers.com 2004
Haastattelu: Ahlroth Riku, IBM Finland
Haastattelu: Heikkilä Olli, toimitusjohtaja, Panorama Partners

Kirjoittaja toimii sovellussuunnittelijana Helsingin kauppakorkeakoulussa.