PALVELUN YLIOPISTOHAKU.FI TIETOTURVA

Yliopistohaku.fi -palvelun toteutuksessa on noudatettu valtionhallinnon tietoturvallisuuden johtoryhmän antamia tietoturvallisuusohjeita sekä julkishallinnon verkkopalveluiden suunnittelun ja toteuttamisen periaatteita. Siten palvelun rakentamisessa on pyritty tietoturvallisuusohjeiden mukaan niin hyvään tietoturvallisuuden tasoon kuin mahdollista.

Palvelun ja asiakkaan tunnistaminen

Palvelussa käytetään sellaisia palvelinvarmenteita, että asiakkaan ei tarvitse epäillä niiden luotettavuutta. Palvelun tunnistaminen edellyttää varmennetta palvelinkoneessa. Palvelua käytetään salatulla yhteydellä (SSL), joka tarkastaa, että palvelimessa oleva varmenne on asiakkaan hyväksymän varmentajan myöntämä ja että se on tarkoitettu kyseiseen palvelinosoitteeseen. Asiakkaan tarvitsee tunnistautua vain käyttäessään tiettyjä järjestelmän palveluja, koska tietoturvallisuusohjeiden periaate on se, että asiakkaan tunnistus tulee tehdä vain tarvittaessa. Asiakkaalta vaaditaan palvelun tietoturvallisen käytön edellyttämää versiota internet-selaimesta.

Käytettävyys ja tietojen eheys

Asiakkaalta kysyttävien tietojen tarpeellisuus on arvioitu suhteessa käyttötarkoitukseen. Mitään sellaista ei kysytä, jota ei tarvita yliopistokoulutukseen haettaessa. Hakulomakkeilla tarjotaan vain ajantasaista tietoa, koska lomake generoidaan tosiaikaisesti tietokannassa olevista ajan tasalle saatetuista tiedoista. Lomakkeen tietojen tarkistukset tehdään välittömästi tietojen syöttämisen jälkeen ja tietojen vastaanoton jälkeen asiakkaalle näytetään kuittausilmoitus.

Selain tallentaa selaimeen haettuja sivuja työaseman levylle sivujen mahdollista uudelleenkäyttöä varten, jotta niitä ei tarvitse (kaikilta osin) hakea alkuperäisestä osoitteesta uudelleen. Välimuisti voi olla tietosuojariski yhteiskäytössä olevilla laitteilla. Palvelussa on ohjeistettu asiakasta tyhjentämään välimuisti, jos järjestelmää käytetään yhteiskäyttöisessä laitteessa.

Asiakkaalle tarjotaan kattava ohjeistus palvelun käyttöön ja pääsy lisätiedon hankkimiseen Opetushallituksen ylläpitämän Koulutusnetin sivuille. Palvelun sivustolla on linkki rekisteriselosteeseen, jossa asiakasta informoidaan henkilötietolain mukaisten tietojen tarkistusoikeudesta.

Nimi- ja osoitetietojen luovuttamisesta asiakkaalta kysytään erikseen suostumus ja rekisteriseloste on osa ohjeistusta. Palvelun ohjesivustolla on linkki tekniseen tietoturvaselosteeseen, jossa asiakasta informoidaan salatun yhteyden käyttämisestä.

Tiedonsiirto

Hakijan palveluun tallentamat tiedot ovat luottamuksellisia ja ne siirretään palveluun salatulla yhteydellä (ratkaisu on SSL). Tietoturvallisuusohjeiden mukaan internet-tiedonsiirrossa on salaamisen käyttäminen suositeltavaa, vaikka kyse olisi pelkästään informatiivisista www-sivuista. Palvelujärjestelmän ja taustajärjestelmien välisten linkkien tietoturvaan on kiinnitetty erityistä huomiota ja ne on rakennettu sellaisiksi, että järjestelmät on eriytetty toisistaan.

Sähköisen palvelun asiakkailla on pääsy vain heille sallittuihin tietoihin.

Sovellusarkkitehtuuri

Sovellusarkkitehtuuri perustuu komponenttipohjaiseen monitasoarkkitehtuuriin. Komponentit ja tasot välittävät tietoa toisilleen palvelupyynnöillä, joissa pyynnön lähde ja sisältö tarkastetaan ennen pyyntöön vastaamista. Esim. palvelujärjestelmästä perusjärjestelmään tulevat palvelupyynnöt on tarkkaan rajattu vain ennalta määrättyihin pyyntöihin. Osa tietoturvallisuuden kannalta keskeisistä toiminnoista on eriytetty omiksi komponenteikseen, joita muut komponentit käyttävät.

TIETOTURVARATKAISUT

Opetushallituksen ylläpitämien nettihakujen (www.yliopistohaku.fi, www.haenyt.fi , www.amkhaku.fi, www.opekorkeahaku.fi ja www.admissions.fi) infrastruktuurin rakentamisessa on huomioitu Valtiovarainministeriön laatimat internetin käyttö- ja turvallisuussuositukset, joissa on kuvattu internetin käytön turvallisuusedellytyksiä.

Verkon rakenne

Tietojärjestelmissä pidetään julkisen verkon kautta tapahtuva toiminta selkeästi erillään organisaation omassa verkossa tapahtuvasta toiminnasta. www-palvelimet on sijoitettu sisäisen verkon ulkopuolelle ja niistä on avattu palomuureihin vain välttämätön tietoliikenneyhteys organisaation tietojärjestelmiin.

Palveluympäristö

Tekninen palveluympäristö on kahdennettu kaikkien kriittisten komponenttien osalta. Internet-yhteydet on toteutettu kahden eri operaattorin kautta, kaikki ympäristöön liittyvät tietoliikenteen aktiivilaitteet (reitittimet ja kytkimet), palomuurit, SSL-kiihdyttimet ja sovelluspalvelimet ovat kahdennettuja. Sovelluspalvelimet sijaitsevat internet-käyttöön suunnitellulla ns. DMZ-alueella ja tietokantapalvelin sijaitsee palomuurin takana toisessa verkossa. Kaikki yhteydet suojattuun verkkoon ja verkosta ulos kulkevat palomuurin kautta ja palomuuriin määritellään, mitä yhteyksiä päästetään läpi.

Liikennöinti internetistä reititetään sovelluspalvelimille kuormantasauspalvelun kautta.

Sovellus vaatii suojattua liikennöintimetodia, joten sovelluksen palvelukutsut pakotetaan SSL-käyttöön redirect-toiminnolla kuormantasaajan toimesta. Palveluympäristössä on SSL-kiihdytinlaitteistot, joiden tehtävänä on muuntaa salattu https-liikenne http-liikenteeksi.