Luottamus. Tietoturva. Sähköiset palvelut.

LUOTI-julkaisuja 3/2006

HABBO WEB

Luotettavien ja turvallisten interaktiivisten palveluiden kehittäminen

LUOTI-pilottihanke
Loppuraportti

Luottamus ja tietoturva sähköisissä palveluissa – kehittämisohjelma

Luottamus. Tietoturva. Sähköiset palvelut.

Sisällysluettelo

Termit ja lyhenteet

Autentikointi	Käyttäjän identiteetin todentaminen: onko käyttäjä se, joka väittää olevansa.
Blogi	Verkkopäiväkirja.
Chat	Reaaliaikainen keskusteluryhmä verkossa.
Haavoittuvuus	Järjestelmän turvallisuuden heikkous, jota hyödyntämällä hyökkääjä voi saada jonkin uhan toteutumaan.
Kertakirjautuminen	Single Sign On; keskitetty käyttäjien tunnistaminen, joka antaa käyttäjän käyttää useita eri palveluja tarvitsematta kirjautua jokaiseen sisään erikseen.
Käytettävyys	Helppokäyttöisyys.
Loki	Tiedosto, johon kirjataan merkintöjä järjestelmän tapahtumista.
Metriikka	Mittari/tilasto.
Moderaattori, moderointi	Habbo Hotellia valvovat hotellin henkilökuntaan kuuluvat moderaattorit, jotka valvovat hotellin sääntöjen noudattamista, auttavat ongelmatilanteissa jne.
OWASP	Open Web Application Security Project; organisaatio jonka tarkoituksena on tunnistaa ja torjua ohjelmistojen turvattomuuden syitä.
Phishing	Phishing (suomeksi myös kalastus tai kalastelu) on rikollista toimintaa, jolla pyritään saamaan haltuun luottamuksellisia tietoja esiintymällä luotettavana tahona, kuten järjestelmän ylläpitäjänä.
Protokolla	Yhteyskäytäntö; määrittelee viestienvaihdon tietoliikenteen osapuolien välillä.
Protokolla-analyysi	Protokollamäärittelyn tutkiminen heikkouksien ja haavoittuvuuksien löytämiseksi.
Scrum	Ketterä ohjelmistokehitysmenetelmä. Perustuu nopeisiin iteratiivisiin pyrähdyksiin, joiden aikana luodaan toimiva versio ohjelmistosta. Asiakas määrää, mitä toiminnallisuutta kehitetään.
Uhka	Ei-toivottu tai vahingollinen asia, joka voisi tapahtua; esimerkiksi järjestelmä ylikuormittuu eikä pysty palvelemaan asiakkaita.

Tiivistelmä

Projekti oli osa LUOTI-ohjelmaa. LUOTI (Luottamus ja tietoturva sähköisissä palveluissa) -ohjelma on liikenne- ja viestintäministeriön tietoturvaohjelma vuosille 2005-2006. Sen tavoitteena on uusien monikanavaisten sähköisten palvelujen tietoturvan kehittäminen.

Habbo Hotelli on erittäin suosittu online-peliympäristö, joka on suunniteltu teini-ikäisille. Sulakkeen tavoitteena on kehittää Habbo Web -hankkeessa web-pohjaista peliympäristöä, joka korvaa nykyisiä peli-client-ratkaisuja ja parantaa pelin elämyksellisyyttä.

Koska Habbo Hotelli on suunnattu alaikäisille, sekä käytettävyys että käyttäjien turvallisuus on erittäin tärkeää. LUOTI-ohjelman asiantuntijapalvelun avulla kehitetään luotettavaa, turvallista ja skaalautuvaa web-peliympäristöä, jonka käytettävyys on korkeatasoista.

Projekti toteutettiin Nixu Oy:n järjestelmäkehityksen turvallisuuden kehittämismallia hyväksikäyttäen. Sulake käyttää Scrum-ohjelmistokehitysmallia, johon Nixu Oy:n lähestymistapaa sovellettiin. Nixu Oy:n menetelmän komponenteista projektissa korostuivat erityisesti tarpeiden määrittelyyn, turvaratkaisun suunnitteluun sekä testauksen suunnitteluun liittyvät tehtävät.

Projektissa tunnistettuja kehitysprosessin tietoturvaongelmia ja -haasteita olivat tietoturvan ja käytettävyyden yhdistäminen, käyttäjien rekisteröinnin, tunnistamisen ja todentamisen turvallisuus, phishing-hyökkäysten torjunta, käyttäjien välisen kommunikoinnin turvallisuus, tietoturvametriikoiden käyttö, tietoturvan testaaminen ja kansainvälisen toimintaympäristön vaatimusten yhteensovittaminen. Näihin ongelmiin projektissa haettiin ratkaisuja ja parhaita käytäntöjä.

1. Yleistä

Habbo Hotelli on online-peliympäristö, joka on suunniteltu teini-ikäisille. Siitä on tullut suosituin ja nopeimmin kasvava teini-ikäisten web-palvelu maailmassa. Tällä hetkellä Habbo-hahmoja on luotu lähes 50 miljoonaa, ja Habbo Hotellissa käy kuukausittain yli 6 miljoonaa erillistä kävijää. Habbo Hotellin tarkoituksena on tarjota uudentyyppistä pelisisältöä, joka on hauskaa, sosiaalista, väkivallatonta ja luovuutta inspiroivaa.

Sulakkeen tavoitteena on kehittää Habbo Web -hankkeessa web-pohjaista peli-ympäristöä, joka korvaa nykyisiä peli-client-ratkaisuja. Hanke parantaa Habbo-elämystä:

- siirtämällä client-pohjaisen ratkaisun elementtejä (mm. rekisteröinti, autentikointi, maksaminen jne.) kehittyneemmille internet-pohjaisille alustoille,
- lisäämällä web-pelaamisen interaktiivisuutta pelaajien välillä,
- kehittämällä uusia web-pohjaisia palveluja (mm. web-radio, käyttäjä-blogit, mini flash -pelit),
- avaamalla pelimaailmaa myös peli-clientin ulkopuolelle webiin, helposti kaikkien nähtäville,
- tarjoamalla oikopolkuja tiettyihin pelin toimintoihin suoraan webistä, jotta erilaiset käyttäjäryhmät löytävät nopeasti omat kiinnostuksen kohteensa.

Koska Habbo Hotelli on suunnattu alaikäisille, sekä käytettävyys että käyttäjien turvallisuus on erittäin tärkeää. LUOTI-ohjelman asiantuntijapalvelun avulla kehitetään luotettavaa, turvallista ja skaalautuvaa web-peliympäristöä, jonka käytettävyys on korkeatasoista.

1.1. Projektin kohde

Projekti oli osa LUOTI-ohjelmaa. LUOTI (Luottamus ja tietoturva sähköisissä palveluissa) -ohjelma on liikenne- ja viestintäministeriön tietoturvaohjelma vuosille 2005-2006. Sen tavoitteena on uusien monikanavaisten sähköisten palvelujen tietoturvan kehittäminen.

Projektin kohteena oli Sulake Corporationin Habbo Web -projekti sen tietoturvaan liittyviltä osin. Habbo Web -hanke sisältää sekä online-/PC-tuotteiden kehittämistä että Sulakkeen sellaisten mobiili-/digitaalisten tuotteiden kehittämistä, joiden avulla parannetaan Habbo-pelin elämyksellisyyttä.

1.2. Projektin tavoitteet ja rajaukset

LUOTI-/Habbo Web -hankkeen päätarkoituksena oli auttaa Habbon kehittäjiä (mukaan lukien kehitykseen osallistuvat alihankkijat) rakentamaan ja ylläpitämään turvallisia yhteisöllisiä web-palveluja sekä luoda ohjeita parhaista käytännöistä uusien palvelujen suunnitteluun. Hankkeessa korostuu tietoturvallisuuden sekä käyttäjä- ja käytettävyys-näkökulman yhdistäminen.

Projektin painopisteet olivat:

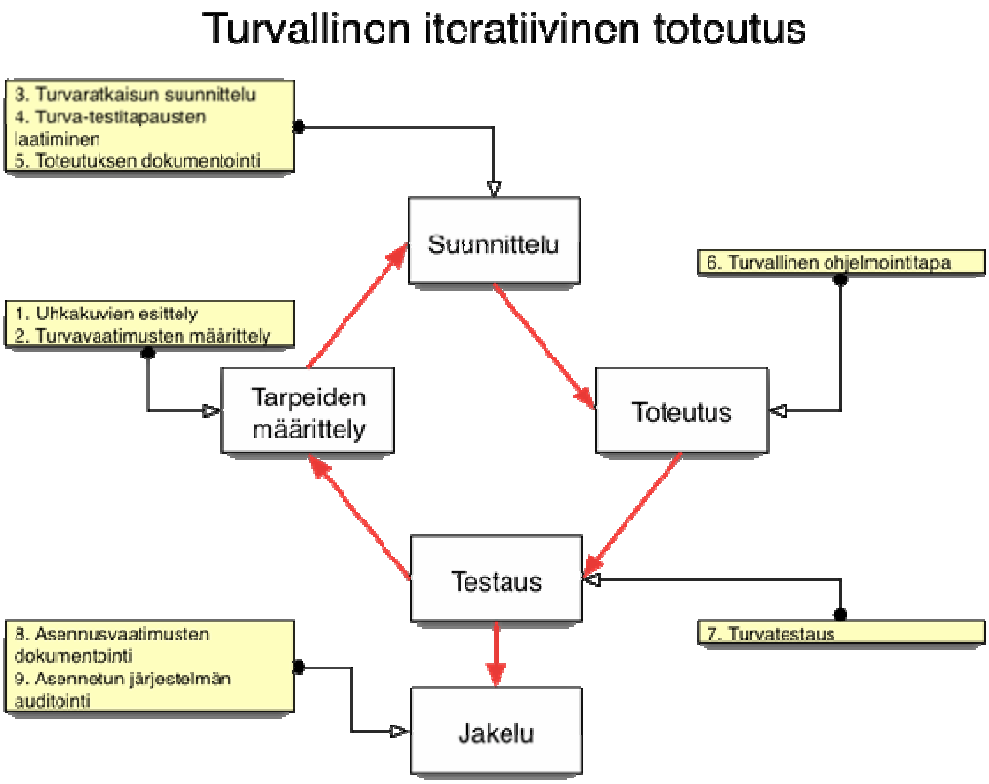
- Käyttäjien rekisteröityminen webissä sekä autentikointi webissä ja mobiilissa.
- Turvallinen käyttäjien välinen viestintä sekä yhdeltä yhdelle (one-to-one-messaging) että yhdeltä monelle (julkiset foorumit sekä käyttäjien oma julkaisutoiminta, kuten blogit).

Projektissa käytiin läpi painopisteisiin liittyvien suunnitelmien tietoturvanäkökulmia pyrkien varmistamaan, että uhkakuvat ja tietoturvavaatimukset on tunnistettu, ja löytämään tunnistettuihin ongelmiin soveliaat ratkaisut. Lisäksi luotiin suosituksia ja ohjeistuksia parhaista käytännöistä tietoturvanäkökohtien huomioon ottamiseksi kehitysprojektin myöhemmissä vaiheissa.

Projektissa ei suoritettu teknisen toteutuksen testaamista, koska hankkeen aikataulusta johtuen projektin kohteena olevien osa-alueiden toteutus ei valmistunut projektin aikana.

1.3. Projektin menetelmät

Projekti toteutettiin Nixu Oy:n järjestelmäkehityksen turvallisuuden kehittämismallia hyväksikäyttäen. Sulake käyttää Scrum-ohjelmistokehitysmallia, johon Nixu Oy:n lähestymistapaa sovellettiin. Nixu Oy:n menetelmän komponenteista projektissa korostuivat erityisesti tarpeiden määrittelyyn, turvaratkaisun suunnitteluun sekä testauksen suunnitteluun liittyvät tehtävät.



Projektin pääasiallisena työmenetelmänä olivat useat työpajatilaisuudet, joihin osallistui Nixu Oy:n konsultin lisäksi henkilöstöä Sulakkeelta sekä Sulakkeen toimittajilta. Työpajatilaisuudet toteutettiin siten, että konsultti piti aluksi valmistellun alustuksen työpajan aiheesta, jonka jälkeen aiheesta käytiin vapaamuotoinen keskustelu alustuksen runkoa löyhästi mukaellen. Tällä tavoin toteutettuna työpajatilaisuudet toimivat paitsi tehokkaana tapana kerätä, analysoida ja jakaa projektin tietoturva-kysymyksiin liittyvää tietoa, myös osallistujien tietoturvatietoisuutta nostavina koulutustilaisuuksina. Projektin keskeisiä painopisteitä käsiteltiin myös LUOTI-hankkeen asiantuntijapoolin työpajatilaisuudessa.

Lisäksi projektissa auditoitiin käyttäjien tunnistamisen nykykäytännöt ja uuden järjestelmän kertakirjautumisratkaisuun liittyvät alustavat suunnitelmat sisältäen eri toteutusvaihtoehtojen protokolla-analyysin.

Koska kysymyksessä oli olemassa olevan palvelun jatkokehitys eikä kokonaan uuden palvelun kehitys, pystyttiin ja toisaalta jouduttiin monissa asioissa tukeutumaan jo aiemmin toteutettujen ratkaisujen varaan.

Projektin tulokset dokumentoitiin asiakkaalle kirjallisesti.

2. Habbo web

2.1. Hankekuvaus

Sulake Corporationin Habbo pyrkii olemaan kaikkein halutuin nuorten yhteisö – osa nuorten jokapäiväistä elämää. Habbo on positiivinen, ystävällinen ja eloisa virtuaalinen kokoontumispaikka, jossa nuoret voivat toteuttaa itseään. Habbo tarjoaa puitteet, ja nuoret ovat itse aktiivisessa roolissa tuottaen ja mukauttaen palvelun sisällön omiin yksilöllisiin tarpeisiinsa sopivaksi. Habbo on nuorille jännä paikka, jossa voi tapahtua paljon erilaisia asioita.

Habbon pääkohderyhmänä ovat 13–16-vuotiaat nuoret, mutta se on tarkoitettu myös vanhemmille leikkimielisille ihmisille. Käyttäjien sukupuolijakauma sisältää noin puolet tyttöjä ja puolet poikia. Käyttäjien kiinnostuksen kohteisiin kuuluvat mm. musiikki, elokuvat, televisio, pelit, tietokoneet, urheilu ja lemmikkieläimet.

Käyttäjät jakautuvat pääkiinnostuksenkohteidensa perusteella kolmeen segmenttiin: sisustuksen ja keräilyn harrastajiin, sosiaalisiin chattaajiin sekä pelaajiin. Käyttäjien tärkein syy Habbo Hotellin käyttämiseen on ystävien tapaaminen ja uusien ystävien löytäminen. Habbo Hotellissa käyttäjät rakentavat omaa identiteettiään ja hakevat muiden hyväksyntää ja arvostusta. Yli puolet käyttäjistä käy Habbo Hotellissa päivittäin. Käyttäjillä voi olla useita Habbo-hahmoja, mutta useimmilla on 1–2 aktiivista Habboa.

Habbo on kansainvälinen palvelukonsepti. Tällä hetkellä aktiivisia Habbo-yhteisöjä on 16 eri maassa eri puolella maapalloa.

Jotta Habbo pysyy nuorille kiinnostavana ympäristönä, täytyy sitä koko ajan kehittää ja lisätä käyttäjille uusia työkaluja. Sulakkeen tarkoituksena on kehittää konseptin kaikkia neljää osa-aluetta: käyttäjien välistä viestintää, käyttäjien identiteetin rakentamista, pelaamista ja viihdettä. Nykyisestä Habbo Hotelli -keskeisyydestä tullaan Habbo Webin palvelujen avulla siirtymään laajempaan Habbo-online-yhteisöön.

Nykyisellään Habbo.com-web-sivusto on lähes puhtaasti markkinointityökalu, jonka kautta voi myös ladata itse Habbo Hotelli -pelin. Varsinainen palvelusisältö on toteutettu Habbo Hotelli -pelissä. Tulevaisuudessa Habbo Web toteuttaa käyttäjien rekisteröitymiseen, tunnistamiseen ja maksamiseen liittyvät perustoiminnallisuudet ja toimii kanavana, jonka kautta on pääsy erilaisiin Habbo-palveluihin, joista Habbo Hotelli on vain yksi esimerkki.

Habbo Web -hanke käynnistyi vuoden 2005 lopussa ja jatkuu vuoden 2006 loppuun. Hankkeeseen liittyvä LUOTI-pilottiprojekti päättyi kuitenkin huhtikuussa 2006, ja kattoi näin ainoastaan Habbo Web -hankkeen alkuosan.

2.2. Habbo web ja tietoturva

Monissa web-palveluissa keskitytään ensisijaisesti torjumaan ulkopuolisten palvelulle mahdollisesti aiheuttamia uhkia, ja käyttäjät mielletään pääosin luotetuiksi tahoiksi. Habbon osalta näin ei kuitenkaan voida toimia, koska kuka tahansa voi rekisteröityä palveluun ilmaiseksi. Osa Habbon käyttäjäkunnasta on tietoteknisesti erittäin taitavaa. Lisäksi kohderyhmän käyttäjät eivät välttämättä vielä osaa hahmottaa, missä kulkee sallitun ja kielletyn käytöksen raja virtuaaliyhteisössä; Habbo Hotelli on peli ja huijaaminen tai ainakin huijauksen yritys kuuluu monen käyttäjän mielestä osaksi pelaamista. Myös Habbo-yhteisöjen suuri koko tekee niistä houkuttelevia hyökkäyskohteita.

3. Tietoturvaongelmat palvelukehitysprosessissa

3.1. Tietoturvan ja käytettävyyden yhdistäminen

Tietoturvaa ja käytettävyyttä/helppokäyttöisyyttä on perinteisesti pidetty toistensa vastakohtina. Liian heikko tietoturva voi kuitenkin heikentää myös palvelun käytettävyyttä esimerkiksi palvelunestotilanteiden kautta. Helppokäyttöisyydestä ei myöskään ole paljoakaan etua, jos käyttäjä ei uskalla käyttää palvelua esim. pelätessään menettävänsä palveluun sijoittamansa rahan. Liian heikko käytettävyys taas vaarantaa tietoturvan, jos käyttäjät eivät ymmärrä, miten palvelun suojausmekanismeja pitäisi käyttää tai aktiivisesti kiertävät liian aggressiivisilta tuntuvia suojausmekanismeja.

Koska Sulakkeen Habbo Hotellin tärkeimpiä ominaisuuksia on miellyttävä käyttäjäkokemus, on käytettävyys- ja turvallisuusnäkökulmat erittäin tärkeä saada yhdistettyä. Käytännössä yhdistäminen tapahtui hankkeessa sekä hakemalla tarkoituksenmukaisia kompromisseja käytettävyys- ja tietoturvatasojen välille että etsimällä uusia käytettävämpiä tapoja toteuttaa aiemmin käytettävyydeltään heikompia tietoturvamekanismeja. Hyvän lopputuloksen saavuttamiseksi on keskeistä, että sekä hankkeen käytettävyydestä että sen tietoturvasta vastaavat henkilöt osallistuvat yhteisiin työpajoihin ja kehittävät ratkaisuja yhdessä.

3.2. Käyttäjien rekisteröinnin ja tunnistamisen turvallisuus

Käyttäjät luovat Habbo Hotelliin rekisteröityessään itselleen Habbo-hahmon. Voidakseen myöhemmin käyttää samaa hahmoa uudelleen käyttäjän on tunnistauduttava palveluun. Lisäksi käyttäjien on mahdollista käyttää rahaa esimerkiksi virtuaalisen huoneen sisustamiseen, jolloin tunnistautumista tarvitaan myös estämään käyttäjiä viemästä toistensa omaisuutta. Tunnistautuminen on kuitenkin ensisijaisesti sidottu yksittäiseen hahmoon eikä käyttäjän todelliseen identiteettiin (periaatteessa ainoat käyttäjän todelliseen identiteettiin liittyvät tiedot ovat syntymäaika ja sähköpostiosoite, ja nämäkin tiedot käyttäjä voi valehdella järjestelmälle). Useilla käyttäjillä onkin käytössään monta hahmoa. Lisäksi alaikäisten käyttäjien yksityisyyden suojaamiseksi palvelu pyrkii estämään käyttäjiä paljastamasta todellista identiteettiään muille palvelun käyttäjille.

Habbo Hotellin käyttäjien tunnistaminen on perinteisesti perustunut käyttäjätunnukseen ja salasanaan. Salasanat ovat monille käyttäjille tuttu menetelmä ja niihin liittyvät investointikustannukset per käyttäjä ovat pienet. Koska Habboa voi käyttää mistä vain ja koska vain, täytyy käytettävän tunnistusmenetelmän olla erittäin laajasti tuettu eikä se saa vaatia käyttäjältä erityistä laitteistoa tai jonkin fyysisen esineen mukana kuljettamista. Vaikka salasanojen käyttöön ja turvallisuuteen liittyy useita

tunnettuja ongelmia, ei niille mm. käyttäjien liikkuvuudesta ja erilaisten päätelaitteiden käytöstä johtuen löydetty kustannustehokasta korvaajaa. Näin ollen projektissa keskityttiin parantamaan salasana-autentikoinnin turvallisuutta ja käytettävyyttä.

Projektin tarkoituksena on siirtää käyttäjien tunnistaminen webiin peli-clientistä, jossa se aikaisemmin toteutettiin. Pelin on jatkossa tarkoitus saada tiedot tunnistautuneista käyttäjistä kertakirjautumisjärjestemän avulla ilman, että käyttäjän tarvitsee syöttää käyttäjätunnusta ja salasanaa uudelleen siirtyessään web-sivulta peliin tai takaisin lyhyen aikavälin sisällä.

Käyttäjien tunnistamiseen liittyen kartoitettiin myös soveltuvia tekniikoita erottaa ihmiskäyttäjät automaateista, jotta voidaan torjua esimerkiksi kampanjaetujen automatisoitua hamstraamista ja hajautettuja palvelunestohyökkäyksiä.

3.3. Phishing

Muun muassa pankkipalveluihin kohdistunut phishing (eli tietojen "kalastelu") on viime aikoina saanut paljon julkisuutta. Habbo Hotellissa phishing-hyökkäykset ovat kuitenkin olleet arkipäivää jo useita vuosia ja niiden käsittelyyn on jo ehtinyt muodostua rutiineja. Phishing-hyökkäyksessä hyökkääjä pyrkii ihmisten hyväuskoisuutta ja teknisiä menetelmiä hyväksikäyttäen huijaamaan käyttäjiä paljastamaan esimerkiksi käyttäjätunnuksensa ja salasanansa, jolloin hyökkääjä pystyy esiintymään uhriksi joutuneena käyttäjänä palvelussa ja esimerkiksi viemään tämän virtuaaliomaisuuden.

Phishing-hyökkäysten torjumisen Habbo Hotellissa tekee haasteelliseksi palvelun nuori kohderyhmä, joka ei välttämättä suhtaudu vakavasti riskiin joutua tällaisen hyökkäyksen kohteeksi eikä jaksa lukea ohjeita ja varoituksia.

Projektin kannalta merkittävin haaste phishing-hyökkäysten torjumisen osalta liittyy kuitenkin palvelussa toteutettaviin muutoksiin. Jotta käyttäjä pystyy välttämään hyökkäyksen uhriksi joutumisen, hänen pitää pystyä erottamaan oikea ja turvallinen sisäänkirjautumistilanne erilaisista huijausyrityksistä. Tähän asti käyttäjiä on järjestelmällisesti opetettu olemaan kertomatta tai syöttämättä salasanaansa mihinkään muualle kuin peliclientin tunnistautumiskyselyyn ja heitä on varoitettu syöttämästä salasanaa esim. erilaisille web-sivuille. Nyt kuitenkin tunnistautumista ollaan siirtämässä peli-clientistä Habbon web -sivustoon, jolloin käyttäjä ei ehkä enää tiedä, mihin salasanan voi turvallisesti syöttää ja mihin ei.

Projektissa kartoitettiin parhaita käytäntöjä phishingin torjumiseksi. Käyttäjien hämmennyksen minimoimiseksi ja käytettävyyden varmistamiseksi muutokset pyritään tekemään asteittain ja tiedottamaan muutoksista hyvissä ajoin.

3.4. Käyttäjien välisen kommunikoinnin turvallisuus

Käyttäjien välinen kommunikointi ja sen turvallisuus on aina ollut keskeinen osa Habbo Hotellia. Tähän asti viestintä käyttäjältä toiselle on ollut pääasiassa chat-tyyppistä. Viestintä on puoliautomaattisesti moderoitua: automaattinen suodatin poistaa viesteistä ei-toivotut sanat ja korvaa ne sanalla "höpö", ja lisäksi hälyttää paikalle Sulakkeen henkilöstöön kuuluvan moderaattorin, mikäli viestintä näyttää sisältävän vaaralliseksi luokiteltuja asioita.

Habbo Web -hankkeessa on kuitenkin tarkoituksena kehittää uusia web-pohjaisia palveluja, jotka tarjoaisivat käyttäjille myös muun tyyppisiä tapoja kommunikoida ja ilmaista itseään. Esimerkkinä näistä uusista palveluista voisivat olla mahdollisesti käyttäjien omat blogit. Tällaisten uusien tapojen ja tekniikoiden mukana tulee kuitenkin myös uusia mahdollisia tapoja hyökätä järjestelmää vastaan.

Projektissa käytiin läpi tyypillisiä tapoja murtaa web-sovellusten turvallisuus ja näiden huomioon ottamista ja torjumista Habbo-palvelussa.

3.5. Tietoturvametriikat ja niiden käyttö

Kokonaan uudenlaisia tietoturvaratkaisuja suunniteltaessa on usein vaikeaa arvioida järjestelmän todellista käyttäytymistä tuotannossa todellisella käyttäjäpopulaatiolla. Pilotointi helpottaa ongelmaa, mutta edustavan käyttäjäpopulaation löytäminen pilottiin saattaa epäonnistua. Lisäksi pilotin perusteella pitäisi pystyä päättelemään, tarvitseeko järjestelmää muuttaa ja jos, niin millä tavalla. Järjestelmän ja käyttäjien käyttäytyminen saattaa myös muuttua ajan myötä.

Jotta tietoturvaa voidaan kehittää joustavasti ja kustannustehokkaasti, on sen toteutus hyvä tehdä parametrisoidusti. Järjestelmän käyttäytymistä voidaan sitten tarkkailla ja mitata ja mittaustulosten perusteella parametreja voidaan säätää halutun lopputuloksen saavuttamiseksi. Oikeiden mittareiden valinta saattaa kuitenkin olla hankalaa. Tämän valinnan helpottamiseksi projektissa tuotettiin ohjeistus tietoturvametriikoiden valinnasta ja käytöstä.

3.6. Tietoturvan testaaminen

Tietoturvan testaaminen eroaa merkittävästi toiminnallisesta testaamisesta. Siinä missä toiminnallinen testaus pyrkii ensisijaisesti varmistamaan, että sovellus toimii määritellyssä tilanteessa määritellyllä tavalla, pyrkii tietoturvatestaus varmistamaan, että sovellus ei toimi millään ei-toivotulla tavalla, joka vaarantaisi järjestelmän tietoturvan. Toisin sanoen, jos toiminnallinen testaus pyrkii tarkastamaan tunnetun

toiminnallisuuden käyttäytyvän halutulla tavalla, pyrkii tietoturvatestaus löytämään ei-tunnetun ja ei-toivotun toiminnallisuuden ja poistamaan sen. Koska tietoturva-vaatimukset on usein ilmaistu negaatioina ("järjestelmä ei tee jotain missään tilanteessa"), niiden kattava testaaminen on vaikeaa ja työlästä.

Käytännössä tietoturvan testaamiseen on muutamia lähestymistapoja, jotka kannattaa yhdistää parhaan lopputuloksen saavuttamiseksi:

- Testataan järjestelmän kestävyyttä vastaavien järjestelmien tunnettuja hyökkäyksiä kohtaan.
- Testataan järjestelmän toimintaa erilaisissa poikkeustilanteissa.
- Katselmoidaan sovelluksen lähdekoodi ja etsitään siitä virheitä, puutteita ja ylimääräistä toiminnallisuutta.

Avainasemassa myös tietoturvatestauksen suhteen on kuitenkin uhkakuvien tunnistaminen sekä kunnollinen vaatimusmäärittely, joihin tietoturvatestauskin perustuu.

Koska tutkimusten mukaan erilaisista yksittäisistä toimenpiteistä lähdekoodin katselmointi parantaa lopputuotteen laatua ja sitä kautta myös tietoturvaa kaikkein tehokkaimmin, luotiin projektissa Sulakkeelle lähdekoodin katselmoinnin ohjeistus. Lisäksi lähdekoodin katselmointi toimintatapana sopii erittäin hyvin ketterän ohjelmistokehityksen ajatusmaailmaan.

3.7. Kansainvälisen toimintaympäristön vaatimukset

Koska Habbo on kansainvälisesti toimiva palvelu, muodostuu eri maiden lainsäädännön vaatimusten yhdistämisestä ja soveltamisesta palveluun merkittävä haaste järjestelmän tietoturvalle, erityisesti tietosuojakysymyksissä. Mm. määräykset siitä, mitä tietoja saa käsitellä, kuka ja miten, miten tietoja on suojattava sekä millaisia ilmoitus-velvollisuuksia palveluntarjoajalla on käyttäjille, vaihtelevat eri maiden välillä. Ongelmaa on pyritty ratkaisemaan mm. minimoimalla käyttäjiltä kerättävän tiedon määrä sekä toteuttamalla kunkin maan lainsäädäntöä lähinnä kyseisessä maassa toimivan Habbo Hotellin osalta. Maakohtaiset räätälöinnit aiheuttavat kuitenkin jonkin verran ylimääräistä työtä ja vaikeuttavat yleispätevien toimintamallien ja ratkaisujen kehittämistä.

Vastaavan tyyppinen ongelma liittyy myös maksujärjestelmiin. Eri maissa ja markkina-alueilla on kullakin omat tyypilliset tavat toteuttaa mikromaksaminen. Lukuisten maksujärjestelmien integroiminen järjestelmään on työlästä ja lisää järjestelmän monimutkaisuutta. Monimutkaisuus taas yleensä lisää tietoturvahaavoittuvuuksien lukumäärää. Lisäksi eri maksujärjestelmien tietoturvan taso vaihtelee, jolloin tietoturva-tasoltaan heikompien menetelmien käyttöönotto lisää väärinkäytösten riskiä

järjestelmässä. Maksujärjestelmien turvallisuuskysymykset eivät kuitenkaan sisältyneet projektin painopistealueisiin.

Eri maiden erilaiset toimintakulttuurit ja säätelykehykset vaikuttavat myös käytännön yhteistyön sujumiseen kolmansien osapuolten kanssa tietoturvaloukkaustilanteita selvitettäessä. Eri maiden operaattorien ja viranomaisten suhtautuminen tietoturva-kysymyksiin vaihtelee suuresti. Esimerkiksi phishing-hyökkäyksiin käytettävän sivuston sulkeminen saattaa jossakin maassa hoitua yhdellä puhelinsoitolla operaattorille, kun taas toisessa maassa vaaditaan viranomaisten, kuten poliisin, puuttumista tilanteeseen.

4. Tietoturva-asioiden ratkaiseminen tuotantoketjussa

Tietoturva ei ole luonteeltaan yksittäinen toimenpide, jonka voisi vastuuttaa tuotantoketjussa yksittäiselle osapuolelle, vaan laatutekijä, joka jokaisen tuotantoketjun osapuolen täytyy ottaa huomioon.

Sulakkeen Habbo Web -projektin tapauksessa tuotantoketju on varsin tiiviisti Sulakkeen omissa käsissä ja hallinnassa. Tuotantoketjuun kuuluu kuitenkin myös muita organisaatioita. Kehitystehtävistä mm. käytettävyyssuunnitteluun osallistuu ulkopuolinen toimittaja ja lisäksi tuotantojärjestelmien palvelualustan isännöinti on ulkoistettu. Suurimman osan toimitusketjun linkeistä Sulake hoitaa itse.

Näin tietoturvavaatimusten huomioiminen kehitystehtävissä kuten ratkaisu-suunnittelussa, testaussuunnittelussa, toteutusvaiheessa sekä tuotantoon viennissä on ensisijaisesti Sulakkeen, mutta myös kehitystehtävissä käytettyjen toimittajien/alihankkijoiden, vastuulla. Vastaavasti palvelualustan tietoturvakysymyksistä huolehtii alustoja ylläpitävä kumppani. Mahdollisten tietoturvaloukkaustilanteiden torjumisessa ja selvittelyssä Sulake toimii tarvittaessa yhteistyössä myös operaattorien ja viranomaisten kanssa, vaikka näiden toimijoiden kanssa ei yleensä ole olemassa sopimussuhdetta.

Loppujen lopuksi vastuu tietoturvaan liittyvistä kysymyksistä on aina palvelun omistajalla, tuotantoketjun monimutkaisuudesta ja osapuolten lukumäärästä riippumatta. Palvelun omistajan tehtävänä on huolehtia, että palvelun tietoturva-vaatimukset ja käytännöt on määritelty ja kommunikoitu hankkeen osallistujille riittävän selkeästi. Omistajan on lisäksi sopimuksien, valvonnan ja jatkuvan kommunikoinnin avulla varmistettava, että kaikki tuotantoketjun osapuolet kantavat oman osuutensa ja vastuunsa palvelun tietoturvasta.

5. Tietoturvaa koskevat menetelmät ja toimintatavat

Normaalisti Nixun järjestelmäkehityksen turvallisuuden kehittämismalli lähtee uhka-analyysistä sekä tietoturvavaatimusten määrittelystä. Tässä projektissa näitä työvaiheita toteutettiin iteratiivisesti kunkin käsiteltävän painopistealueen osalta sikäli, kun Sulake ei ollut jo itse toteuttanut näitä tehtäviä.

5.1 Käyttäjien tunnistaminen

Käyttäjien tunnistamiseen liittyviä tietoturvanäkökohtia oli Sulakkeessa mietitty paljon jo aiemminkin. Järjestelmän tietoturvallisuuden ja käytettävyyden parantamiseksi tehtiin katselmoinnin perusteella kuitenkin mm. seuraavat suositukset:

- Salasanojen maksimipituutta olisi pidennettävä. Käyttäjien on helpompi muistaa itselleen merkityksellisiä lauseita kuin yksittäisiä sanoja ja lisäksi pitemmän salalauseen murtaminen raa'alla voimalla vaatii selkeästi enemmän vaivaa kuin lyhyen salasanan.
- Käyttäjiä pitäisi edellyttää tunnistautumaan palveluun uudelleen pidempään jatkuneen toimettomuuden jälkeen.
- Käyttäjille olisi tarjottava selkeä uloskirjautumistoiminto. Tämä on erityisen tärkeää sen jälkeen, kun uusi kertakirjautumistoiminto otetaan käyttöön, jotta käyttäjän istunto ei vahingossa jää avoimeksi esimerkiksi yhteiskäyttöiselle tietokoneelle kirjastossa tai koulussa.
- Käyttäjien ohjeistusta pitäisi edelleen kehittää.
- Tunnistautumissivun URL:in pitäisi olla helppo ja yksinkertainen, jotta käyttäjän on helpompi varmistaa olevansa oikeassa paikassa ennen käyttäjätunnuksen ja salasanan syöttämistä.
- Luottamuksellista tietoa sisältävä kommunikointi käyttäjän selaimen ja Habbo.com-palvelimen välillä olisi salattava.

Lisäksi protokolla-analyysin perusteella suositeltiin toteutettavaksi CAS 2.0 -protokollamäärittelyä melko tarkasti noudattelevaa vaihtoehto numero 1:tä, joka oli esitetyistä vaihtoehdoista yksinkertaisempi eikä sisältänyt erillistä peli-istuntotunnistetta CAS-pääsylipun lisäksi käyttävässä 2. vaihtoehdossa havaittua haavoittuvuutta.

5.2 Lähdekoodin katselmointi

Jos ohjelmistokehityksen lopputuloksen laadun ja sitä kautta myös tietoturvan kehittämiseksi täytyisi valita tehokkain yksittäinen toimenpide, se olisi koodin katselmointi. Sovelluksen kehittäjille toteutettiin projektissa lähdekoodin katselmointi-ohje, jotta katselmoinnit olisi helpompi ja tehokkaampi toteuttaa.

Lähdekoodin katselmoinnin pitäisi aina suorittaa joku muu kuin koodin alkuperäinen kirjoittaja/kirjoittajat. Katselmoijalla olisi kuitenkin oltava riittävät tiedot kehitettävästä ohjelmistosta, kehitysvälineistä ja tietoturvasta. Kaikki lähdekoodi pitäisi katselmoida ennen tuotantoon vientiä vähintään automaattisia työkaluja käyttäen ja kriittisiltä osin myös manuaalisesti.

Lähdekoodin katselmoinnin olisi tarkasteltava lähdekoodia ainakin seuraavien avainkysymyksien osalta:

- Täyttääkö ohjelmisto sille asetetut vaatimukset? Sisältääkö ohjelmisto ylimääräistä toiminnallisuutta?
- Onko käytetty koodaustyyli selkeä ja ohjeiden mukainen? Löytyykö merkkejä "leikkaa-liimaa" -ohjelmoinnista?
- Onko koodi kunnolla kommentoitu?
- Onko koodissa tavallisia tietoturvavikoja? Tietoturvavikalistana kannattaa käyttää esimerkiksi OWASP:in Top Ten -listaa tai listaa ohjelmistokehityksen "19 kuolemansynnistä".

Varsinkin kokemattomamman katselmoijan kannattaa katselmointia suorittaessaan keskittyä vain yhteen tai muutamaan edellä mainituista kysymyksistä kerrallaan, jottei mitään oleellista jäisi vahingossa huomaamatta.

5.3 Tietoturvan mittaaminen

Tietoturvan järjestelmällinen mittaaminen auttaa hallitsemaan palvelun todellista tietoturvatasoa ja tietoturvamekanismien toimintaa. Oikein valittujen mittarien avulla voidaan myös ennakoida tulevaa ja varautua toimenpiteisiin jo ennen kuin muutoksella on ollut merkittävä haittavaikutus liiketoiminnalle. Oikean tiedon tehokas kerääminen vaatii kuitenkin toimenpiteitä jo palvelun kehitysvaiheessa sopivien lokidatankeräys-mekanismien toteuttamiseksi. Lisäksi mittarin seuraamisessa kannattaa varmistaa, että eri aikoina kerätyt mittaustulokset ovat keskenään vertailukelpoisia, jotta kehitys-suuntien analysointi on mahdollista.

Palvelun tietoturvan seuraamiseksi ja mittaamiseksi toteutettiin suositus, jonka tavoitteena oli auttaa kehittäjiä valitsemaan järjestelmästä kerättävät tiedot sekä kertoa, miten näitä tietoja kannattaa käyttää hyväksi. Yleisperiaatteena on, että tietoa, jota ei käytetä mihinkään, ei kannata kerätä – mittauksen on kohdistuttava asioihin, joilla on merkitystä järjestelmän tietoturvavaatimusten kannalta.

Hyödyllisiä palvelun tietoturvaa koskevia mittareita ovat mm.

- Järjestelmän yleinen suorituskyky. Järjestelmän epätavallinen suorituskyky saattaa olla ensimmäinen vaaran merkki esimerkiksi virusepidemiatilanteessa. Lisäksi heikko suorituskyky saattaa altistaa järjestelmän palvelunestohyökkäyksille.
- Käyttäjien tunnistamiseen ja istunnonhallintaan liittyvät mittapisteet (sisään- ja uloskirjautumiset, istuntojen katkaisut, salasanojen vaihdot ja resetoinnit sekä virhetilanteet). Näiden tietojen perusteella voidaan säätää järjestelmän asetuksia siten, että suojauksen painoarvoa siirretään huonosti toimivilta mekanismeilta tehokkaammille menetelmille.
- Järjestelmän tapahtumien kirjausketju (audit trail). Erityisesti rahaa tai muuta rahanarvoista materiaalia käsittelevien sovellusten täytyy kerätä tapahtumista riittävästi tietoa, jotta väärinkäytökset voidaan tutkia ja analysoida. Näin muodostuvaa tapahtumaketjua (eli audit trailia) analysoimalla on myös mahdollista luoda kuva käyttäjien tyypillisestä tavasta toimia, jolloin väärinkäytökset on helpompi havaita (esimerkiksi jos innokas keräilijä yhtäkkiä alkaa luovuttaa omaisuuttaan pois kovaa vauhtia).
- Toteutuneiden tietoturvaloukkausten ja "läheltä piti" -tilanteiden syistä ja seurauksista pidettävä kirjaus. Auttaa priorisoimaan tietoturvan kehityshankkeet todellisten tarpeiden mukaisesti.
- Järjestelmän vaatimustenmukaisuus sekä omien että ulkoisten vaatimusten osalta (jos sellaisia on). Tyypillisiä omien tietoturvavaatimusten mittareita ovat esim. asentamattomien tietoturvapäivitysten määrä sekä järjestelmien kovetuksen kattavuus. Vaatimustenmukaisuuden ajoittainen mittaaminen saattaa jopa kuulua itse vaatimuksiin. Auttaa priorisoimaan tietoturvan kehityshankkeet todellisten tarpeiden mukaisesti sekä valvomaan tarvittaessa palveluntarjoajan sopimuksen palvelutasosopimuksen noudattamista.

6. Johtopäätökset

Toimeksiannon tarkoituksena oli tarjota Habbo Webin kehitystiimille asiantuntevaa sparrausapua tietoturvallisten, käytettävien ja yhteisöllisten web-palvelujen kehittämiseen ja erityisesti auttaa kehittäjiä huomioimaan tietoturvakysymykset hankkeen kaikissa vaiheissa aivan alusta saakka. Tällä tavalla pyritään varmistamaan riittävän tietoturvatason mahdollisimman kustannustehokas toteuttaminen.

Hankkeen aikana on tunnistettu mm. käyttäjien tunnistukseen ja käyttäjien väliseen kommunikointiin liittyviä tietoturvauhkia ja vaatimuksia sekä kartoitettu sopivia ratkaisumalleja. Salasana-autentikoinnin saamisesta mahdollisimman turvalliseksi toteutettiin nykytila-analyysi ja kuvattiin sen perusteella suositukset kehitystoimenpiteiksi. Kertakirjautumisen eri toteutusvaihtoehtojen protokollat analysoitiin ja esitettiin suositus ratkaisun valinnaksi. Phishing-hyökkäysten torjuntaan, web-sovellusten tavallisten tietoturvaongelmien tunnistamiseen ja torjuntaan, tietoturvametriikoiden soveltamiseen sekä lähdekoodin katselmointiin kuvattiin parhaita käytäntöjä ja suosituksia.

Tietoturva, niin kuin käytettävyyskin, ei ole ainoastaan määriteltyä toiminnallisuutta, vaan kaikkeen ohjelmistokehitykseen liittyvä laatutekijä – kokonaisuuden tietoturva on yhtä vahva kuin sen heikoin lenkki. Tämän vuoksi tietoturvaa ei myöskään voida kokonaisuudessaan vastuuttaa yksittäiselle kehityshankkeen osapuolelle, vaan jokaisen osapuolen on omalta osaltaan edesautettava halutun tietoturvatason saavuttamista.

LUOTI-projektin tuloksena voidaan sanoa, että tietoturvakysymyksien käsittelyyn kannattaa ottaa mukaan ihmisiä erityyppisistä rooleista. Näin varmistetaan, että kukin osapuoli on ymmärtänyt oman vastuunsa tietoturvallisen lopputuloksen synnystä. Lisäksi eri näkökulmia edustavien ihmisten yhteistyönä voidaan löytää tavat yhdistää jopa joissain tilanteissa päällepäin ristiriitaisilta vaikuttavia vaatimuksia, kuten tietoturva ja käytettävyys.

Kokonaisuudessan Habbo Web -hanke, johon tämä LUOTI-pilottiprojekti liittyi, ei ole vielä edes puolivälissä. Siksi on vielä hieman aikaista arvioida projektin vaikutusta hankkeen lopputulokseen ja kustannuksiin. Habbo Webin kehitystiimi koki silti projektin osoittautuneen hyödylliseksi jo tässä vaiheessa. Habbo Web -hankkeen lisäksi monia projektissa käytettyjä toimintamalleja sekä tuotettuja suosituksia ja neuvoja voi soveltaa myös tulevissa kehityshankkeissa.