Luottamus. Tietoturva. Sähköiset palvelut.

LUOTI-julkaisuja 2/2006

VAHINKOLAUKAUKSIA

Luotettavien ja turvallisten interaktiivisten palveluiden kehittäminen

LUOTI-pilottihanke
Loppuraportti

Luottamus ja tietoturva sähköisissä palveluissa – kehittämisohjelma

Luottamus. Tietoturva. Sähköiset palvelut.

Sisällysluettelo

Sisällysluettelo 3

Kuvat ja taulukot 4

Termit ja lyhenteet 5

Tiivistelmä 6

1. Yleistä 7

1.1. Taustaa 7

1.2. Projektin kohde 8

1.3. Projektin tavoitteet 9

1.4. Projektin menetelmät 11

1.4.1. Työmenetelmät 11

1.4.2. Projektin vaiheet ja tuotokset 11

2. New Media, New Millenium (NM2) -järjestelmä 13

2.1. NM2-järjestelmän käyttö Vahinkolaukauksia-tuotannossa 14

3. Tietoturvan huomioiminen Vahinkolaukauksia-hankkeessa 15

3.1. Palveluprosessin ja käyttötapausten kuvaaminen 15

3.2. Tietoturvavaatimusten kuvaaminen 17

3.3. Tietoturvariski- ja uhka-analyysin kuvaaminen 18

3.4. Tietoturva-arkkitehtuurin kuvaaminen 19

3.5. Testaus- ja auditointisuunnittelu 21

3.6. Tietoturvatavoitteiden kuvaaminen 22

3.7. Merkittävimmät esille tulleet tietoturvakysymykset 24

4. Tietoturvan ratkaiseminen tuotantoketjussa 26

4.1. Palvelun tuotanto ja roolit 26

5. Johtopäätökset 28

Lähdeviitteet 30

Kuvat ja taulukot

Kuva 1. Luonnos Vahinkolaukauksia-TV-grafiikasta. Vahinkolaukauksia-ohjelmassa vaikutetaan mobiiliviestinnän keinoin ohjelman kulkuun. 8

Kuva 2. Projektissa sovellettu työmenetelmä osoittautui tehokkaaksi. 11

Kuva 3. NM2-järjestelmä muodostuu mediatuotantoon ja -jakeluun tarkoitetuista työkaluista. 13

Kuva 4. Jakelujärjestelmä tarjoaa useita eri kanavia NM2-järjestelmään. 14

Kuva 5. Prosessikartta Vahinkolaukauksia-hankkeeseen liittyvistä prosesseista. 15

Kuva 6. Käyttötapauskaavio ”Broadcasting and Mobile Interaction”. 16

Kuva 7. NM2-järjestelmän looginen arkkitehtuuri Vahinkolaukauksia-tuotannossa. 20

Kuva 8. Vahinkolaukauksia-hankkeessa on useita arvoketjun osapuolia. 26

Taulukko 1. Vahinkolaukauksia-hankkeessa esille tulleet tietoturvakysymykset. 24

Termit ja lyhenteet

Aktori	Toimija. Toimija on prosessikuvauksissa aktiviteetin suorittaja.
AL	Accidental Lovers. AL on englanninkielinen käännös Vahinkolaukauksia-tuotannolle.
API	Application Programming Interface. API on ohjelmointirajapinnan kuvaus.
BPMN	Business Process Modeling Notation. BPMN on liiketoimintaprosessin kuvausformaatti.
EU	European Union. EU on Euroopan maiden muodostama yhteisö.
FP	Frame Programme. FP on EU:n kuuden vuoden välein julkistama puiteohjelma tutkimus- ja kehityshankkeille.
IAMC	InterActive Media and Consultancy. IAMC on TietoEnatorin konsulttiyksikkö Media-yksikössä.
Indigo	Indigo on digitaalisen median käsittelyyn ja lähettämiseen tarkoitettu laitteisto.
IST	Information Society Technology. IST on EU:n meneillään olevaan puiteohjelmaan kuuluva ohjelmakokonaisuus, jossa painotetaan teknologiaratkaisuja monimedia-alaiselle viihdesisällölle.
LUOTI	Luottamus, tietoturva ja sähköiset palvelut. LUOTI on liikenne- ja viestintäministeriön kehittämisohjelma, jossa haetaan ratkaisuja siihen, miten tietoturva tulisi ottaa huomioon palvelukehityshankkeissa.
LVM	Liikenne- ja viestintäministeriö.
Middleware	Välityskerros. Välityskerroksen tehtävä ohjelmistoarkkitehtuurissa on erottaa asiakasrajapinta palvelukerroksen toteutuksesta.
NM2	New Media for a New Millenium. NM2 on EU-projekti, jossa kehitetään työkaluja uudentyyppisen mediasisällön tuottamiseen.
RUP	Rational Unified Process. RUP on ohjelmistokehitysmenetelmä.
SDI	Serial Digital Interface. SDI on digitaalisen kuva- ja ääniaineiston lähetysformaatti.
SRM	Security Requirements Management. SRM on TietoEnatorilla kehitetty tietoturvavaatimusten hallintamenetelmä ohjelmistokehityshankkeissa.
TAIK	Taideteollinen Korkeakoulu.
TE	TietoEnator.
TE Object	TietoEnator Object. TE Object on TietoEnatorilla kehitetty ohjelmistokehitysmenetelmä.
UIAH	University of Art and Design Helsinki. UIAH on englanninkielinen käännös Taideteolliselle Korkeakoululle.
UML	Unified Modeling Language. UML on kuvausmenetelmä ohjelmistokehityksessä käytetyille diagrammeille ja kuvauksille kuten sekvenssikaaviot ja luokkamallit.

Tiivistelmä

Liikenne- ja viestintäministeriön LUOTI-ohjelman tavoitteena on uusien monikanavaisten sähköisten palvelujen tietoturvan kehittäminen edistämällä uusien toimintamallien kehittymistä. Ohjelman asiantuntijapalvelujen toimintamallissa tietoturva otetaan huomioon sähköisten palvelujen kehittämisen alkuvaiheessa. Ohjelma on kaksivuotinen ja ajoittuu vuosille 2005 ja 2006.

LUOTI-ohjelmaan valittiin vuonna 2005 kolme pilottihanketta, joihin tässä raportissa esitelty Vahinkolaukauksia kuului.

Ohjelman pilottihankkeiden yrityksillä on mahdollisuus käyttää asiantuntijapoolin tarjoamaa tietoturva-asiantuntijapalvelua yritysten palvelukehityshankkeiden suunnittelussa, verkoston ohjaamisessa, auditoinnissa ja seurannassa sekä raportoinnissa.

LUOTI-ohjelmaan valittiin vuoden 2005 lopulla Vahinkolaukauksia-hanke, jonka osapuolina on Taideteollisen Korkeakoulun Mediakeskus Lumen Crucible Studio, jolle tietoturva-asiantuntijapalvelua tarjosi TietoEnatorin Telecom & Media -alueelta Media-yksikön InterActive Media and Consultancy (IAMC) -ryhmä. Muissa rooleissa hankkeessa oli YLE ja operaattoripalveluja tarjoavat tahot.

Vahinkolaukauksia-hankkeessa tutkitaan, miten televisiodraamaa voidaan tuottaa siten, että katsojilla on mahdollisuus vaikuttaa ohjelman kulkuun lähetysaikana tekstiviestejä lähettämällä.

Keskeisimpiä tietoturva-asioita hankkeessa oli käytettävyys, turvattu laskutus, jakelumekanismit, käyttäjätiedon turvaaminen, interaktiivisen palvelun luotettavuus sekä tuotantoympäristön turvaaminen.

1. Yleistä

1.1. Taustaa

LUOTI on liikenne- ja viestintäministeriön tietoturvaohjelma vuosille 2005 ja 2006. Sen tavoitteena on uusien monikanavaisten sähköisten palvelujen tietoturvan kehittäminen. LUOTI-ohjelmaan valittiin vuonna 2005 kolme pilottihanketta, joihin Vahinkolaukauksia-hanke kuului. Painopiste pilottihankkeita valittaessa oli viihde.

Pilottihankkeiden tavoitteena oli käytännön avulla kehittää uutta toimintamallia, jossa tietoturva otetaan sähköisiin palveluihin mukaan jo niiden kehittämisen alkuvaiheessa. Lopullisena tavoitteena on kuluttajien luottamuksen lisääminen uusiin sähköisiin palveluihin.

LUOTI-ohjelma tarjosi pilottihankkeiden käyttöön tietoturva-asiantuntemusta pilotissa kehitettävän palvelun suunnitteluun, kehittämisen tueksi sekä auditointiin. Vahinkolaukauksia-hanke valitsi LUOTI-ohjelman asiantuntijaryhmästä tietoturva-asiantuntijaksi TietoEnator Telecom & Median. Vahinkolaukauksia-hanke on osa EU:n kuudennen puiteohjelman IST NM2 -tutkimus- ja kehitysprojektia, joka ajoittuu vuosille 2004-2007. Taideteollinen Korkeakoulu vastaa Vahinkolaukauksia-hankkeen taiteellisesta tuotannosta ja NM2-partnerit teknisestä toteutuksesta.

Vahinkolaukauksia-hankkeen keskeisimmät osapuolet LUOTI-ohjelmassa ja näiden roolit:

- TietoEnator, joka vastasi projektin suunnittelusta, avusti prosessi- ja konsepti-kehityksessä sekä vastasi tietoturvaratkaisun kehittämisestä. TietoEnatorilta tähän osallistuivat konsultit Kimmo Rytkönen ja Kari Tiihonen.
- Taideteollinen Korkeakoulu, joka vastasi projektin hallinnasta, edusti Vahinkolaukauksia-tuotantoa, ja kommunikoi NM2-projektin suuntaan LUOTI-hankkeen tuotoksista sekä vastasi projektin tulosten katselmoinnista. Taideteollisesta Korkeakoulusta projektiin osallistuivat tuottaja Paavo Häikiö ja tekninen asiantuntija Topias Marttila.
- NM2-projektin osapuolet huomioivat LUOTI-hankkeen tulokset NM2-järjestelmä-kehityksessä sekä sen testausvaiheessa.
- YLE, joka vastaa Vahinkolaukauksia-tuotannon lähetyksestä. YLEltä projektiin osallistui tietoturvapäällikkö Janne Huhtakallio, joka avusti tietoturva-asioiden käsittelyssä.

1.2. Projektin kohde

NM2 on meneillään oleva EU-projekti (2004-2007), jossa tutkitaan ja kehitetään uusia kerronnan muotoja sekä työkaluja uudentyyppisen mediatuotannon käyttöön. Tällä tarkoitetaan käyttäjälähtöistä mediatuotantoa, jossa katsoja voi vaikuttaa siihen, mitä hän näkee ja kuulee. Tällaisen personoidun mediakokemuksen mahdollistaa käytettävissä oleva teknologia, kuten laajakaistayhteydet, suuri tallennuskapasiteetti ja oliopohjainen mediaelementtien käsittely. NM2-projektissa tuotettavia työkaluja pilotoidaan eri mediatuotannoissa, kuten uutisraportoinnissa, dokumenttituotannossa ja interaktiivisessa televisiotuotannossa. NM2-tutkimushankkeen tulokset eivät ole kaupallisia, ellei jokin hankkeen osapuoli sitä halua erikseen tehdä.

Vahinkolaukauksia (engl. Accidental Lovers) – tutkimustuotanto on yksi NM2-projektin pilotti, jossa kehitetään vuorovaikutteista, televisiossa esitettävää keskustelu- ja mustan huumorin sarjaa rakkaudesta (kuva 1).

Sarja esittelee uuden interaktiivisen formaatin ja lajityypin televisio-ohjelmalle. Ohjelman katsoja pystyy vaikuttamaan ennalta arvaamattoman draaman kulkuun ja sen käänteisiin lähettämällä tekstiviestejä. Tekstiviestit käsitellään järjestelmässä, jossa ne vaikuttavat draaman etenemiseen tekstiviestien avainsanatunnistuksen keinoin. Interaktiivisuus ilmenee siinä, että lähetetyt tekstiviestit ja näiden perusteella muodostettu taustakerronta näytetään katsojille. Ohjelman lähetyksen aikana lähetetyt tekstiviestit vaikuttavat kumulatiivisesti draaman kulkuun.

Kuva 1. Luonnos Vahinkolaukauksia-TV-grafiikasta. Vahinkolaukauksia-ohjelmassa vaikutetaan mobiiliviestinnän keinoin ohjelman kulkuun.

Draama koostetaan dynaamisesti NM2-järjestelmään lähetettyjen tekstiviestien perusteella. Järjestelmä hyödyntää laajaa multimediatietokantaa, johon on tallennettu

etukäteen ohjelman käsikirjoituksen mukaan erilaiset draaman etenemismallit video- ja audiomateriaaleineen. Video- ja audiomateriaaliin on etukäteen liitetty metatietoa, mikä samalla määrää, mitkä multimediaobjektit voivat liittyä toisiinsa, jotta draaman eteneminen on tarinankerronnallisesti looginen. Avainsanat on linkitetty audiomateriaaliin, josta valitaan lähetykseen materiaalia tekstiviestien avainsana-tunnistuksen perusteella. Käytännössä tämä tarkoittaa sitä, että ohjelmaformaattia voidaan lähettää televisiossa useita kertoja niin, että draaman juoni vaihtelee sen mukaan, miten katsojat reagoivat ja haluavat tarinan etenevän.

Edellä kuvatuin keinoin voidaan toteuttaa uutta personoitua ja tarvepohjaista lajityyppiä myös laajakaistaohjelmaformaatille. EU:n NM2-projektissa kehitettävillä tuotanto-työkaluilla voitaisiin käsitellä mediasisältöä ja liittää se personoituun tarinaan. Näin digitaalisia formaatteja hyödyntävästä mediatuotannosta saadaan käyttäjälähtöisempi kokemus, joka on interaktiivisempi ja personoidumpi kuin perinteinen yhteisöllinen mediatuotanto tähän mennessä.

EU-projektin tavoitteena on muuttaa perinteistä käsitystä passiivisesta mediakäyttäjästä, joka ei voi vaikuttaa median sisältöön tai siihen, mitä hän näkee ja kuulee. Projektissa tuotetaan NM2-järjestelmän työkaluja yhteensä seitsemälle eri tuotannolle:

- City Symphonies
- Gods In The Sky
- Gormenghast
- Runecast
- MyNews&SportMyWay
- Accidental Lovers
- A Golden Age

Projektiin osallistuu kaikkiaan 13 osapuolta mm. operaattoreita, mediatuotantoa ja tutkimuslaitoksia kahdeksasta Euroopan maasta.

1.3. Projektin tavoitteet

LUOTI-ohjelman tavoitteena on monikanavaisten sähköisten palvelujen tietoturvan edistäminen ohjelmassa luotavan toimintamallin avulla. Toimintamallin päälinjaukset tietoturva-asiantuntijapalvelussa määriteltiin yritysten palvelukehityshankkeille LVM:n tarjouspyynnössä.

Tietoturva-asiantuntijan tarjoaman toimituksen sisältö piti muodostua tietoturva-palvelusta, joka ottaa huomioon toimintamallin päälinjaukset. Toimintamallin käyttö sovittiin erikseen pilottihankkeiden tarpeiden mukaan. Toimitukseen piti liittyä seuraavat tunnistettavat vaiheet ja tehtävät:

- Suunnitteluvaihe, jonka tavoitteena on kartoittaa pilottihankkeen tietoturva-asiat ja esittää ratkaisu niiden toteuttamiseksi palvelukehityksen eri vaiheissa.
- Verkoston ohjaamisen vaihe, jonka tehtäviin kuuluu palvelun tuotantoketjun, johon voi kuulua erilaisia osapuolia kuten järjestelmätoimittaja, alihankkija, operaattori, sekä laitetoimittaja, edustajien konsultointi ja ohjaus sekä suunnitelman esittäminen tuotantoketjun osapuolten rooleista tietoturva-alueiden ratkaisemisessa.
- Auditointi- ja seurantavaihe, jonka aikana auditoidaan kehitettävä palvelu joko sen testaus- tai käyttöönottovaiheessa.
- Raportointivaihe, jossa raportoidaan LUOTI-ohjelmalle pilottihankkeessa kehitetyn palvelun aikana syntyneistä tuloksista tietoturvan osalta (mm. tietoturvatoimintatavat).

TietoEnatorin tarjoama toimintamalli perustuu TietoEnatorin TE Object -ohjelmistokehitysmalliin sekä TietoEnatorilla kehitettyyn SRM (Security Requirements Mapping) -tietoturvavaatimusten käsittelymalliin.

TE Object on tarkoitettu liiketoiminnan kehittämiseen, kehityssuunnitelmien laatimiseen, tietojärjestelmien määrittelyyn, suunnitteluun, toteutukseen, testaukseen ja käyttöönottoon. Kehitystyömalli ottaa huomioon tietoturva-asiat tietojärjestelmien kehittämisen eri vaiheissa. Tätä mallia on soveltuvin osin hyödynnetty tässä projektissa.

SRM on prosessikuvaus erityisesti tietoturvavaatimusten hallintaan. Sitä voidaan hyödyntää osana laajempaa ohjelmistokehitysmallia, kuten TE Object tai RUP.

Toimintamalli ottaa kantaa kehitettävän palvelun tietoturva-asioiden kartoitukseen, ja suunnitelmalliseen ratkaisemiseen palvelun kehittämisen eri vaiheissa. Toimintamalliin liittyy tietoturvasuunnitelma, joka määrittää toteutuksen eri osa-alueiden vastuut ja roolit. Toimintamalli palvelee myös kehitettävän palvelun tietoturva-auditointia sen testaus- ja käyttöönottovaiheissa. Toimintamallia sovellettiin osana Vahinkolaukauksia-hanketta.

1.4. Projektin menetelmät

Toimintamallin sisältämiä vaiheita ja niihin sisältyviä työmenetelmiä sekä tuloksia kuvataan seuraavissa kappaleissa. Vaiheiden toteutusta sovellettiin Vahinkolaukauksia-tuotannon ja sen hetkisen NM2-projektitilanteen mukaan.

1.4.1. Työmenetelmät

Projektin suunnitteluvaiheessa päädyttiin noudattamaan projektimenetelmää, jossa yhteisiä asioita käsitellään ja projektin tuotoksia jalostetaan yhteisissä päivän kestävissä työpalavereissa (kuva 2). Projektin tehokkaan etenemisen ja kommunikoimisen vuoksi keskeisimmät henkilöt olivat aina paikan päällä.

TietoEnatorin vastuulla oli valmistella työpalaverit, luoda alustavat konseptikuvat ja kuvaukset hyödyntäen olemassa olevaa aineistoa. Työpalavereissa alustava dokumentaatio tarkastettiin, katselmoitiin ja muutokset kirjattiin ylös. Ennen seuraavaa työpalaveria TietoEnator valmisteli uudet versiot dokumentaatiosta ja toimitti ne asiakkaalle kommentoitavaksi. Työpalavereissa hyväksyttiin lopulliset versiot dokumentaatiosta.

Kuva 2. Projektissa sovellettu työmenetelmä osoittautui tehokkaaksi.

1.4.2. Projektin vaiheet ja tuotokset

Projektin suunnitteluvaiheessa sovittiin projektin tehtävistä sekä työpalaverit ja niissä käsiteltävät asiat. Suunnittelussa otettiin huomioon se, että NM2-projektissa Vahinkolaukauksia-hankkeen tuotantokuvaukset sekä vaatimukset oli jo kuvattu ja sovelluskehitys tuotantotyökalujen osalta oli meneillään. Kehitettävät tuotantotyökalut oli tarkoitettu kaikille seitsemälle NM2-projektissa kehitettävälle tuotannolle, joten mitään työkalua ei kehitetty yhden tuotannon tarpeita varten. Siitä huolimatta tuotanto-työkalujen toiminnallisuuksiin pystyi vielä tässä vaiheessa vaikuttamaan. Sovelluskehityksessä tietoturva-aktiviteetit oli tarkoituksella jätetty pois, koska ne eivät mahtuneet NM2-projektiin.

Tältä pohjalta työpalaverit jaettiin niin, että seuraavat asiat tulisi määriteltyä ja dokumentoitua Vahinkolaukauksia-hankkeen sovelluskehityksen tilanne huomioiden:

- Palveluprosessit ja järjestelmän käyttötapaukset
- Järjestelmän tietoturvavaatimukset
- Tietoturvariski- ja uhka-analyysi
- Tietoturva-arkkitehtuuri
- Testaus- ja auditointisuunnitelma
- Tietoturvatavoitteet

Palveluprosessin kuvaamisella pyrittiin hahmottamaan järjestelmän osia ja tiedon kulkua järjestelmässä sekä tunnistamaan tietoturvan kannalta keskeisimmät prosessin osat. Taustamateriaalina prosessikuvauksia laadittaessa käytettiin NM2-projektin teknisiä määrittelyjä. Palveluprosessin laatimista on kuvattu kappaleessa ”**Palveluprosessin ja käyttötapausten kuvaaminen**”.

Palveluprosessin kuvauksista johdetuilla käyttötapauksilla tarkennettiin järjestelmän käyttöä, tunnistettiin poikkeustilanteet ja listattiin alustavia tietoturvavaatimuksia. Käyttötapausten laatimista on kuvattu kappaleessa ”**Palveluprosessin ja käyttötapausten kuvaaminen**”. Tietoturvavaatimuksia käytiin läpi valmiiden prosessikuvausten ja käyttötapausten pohjalta erillisessä työpalaverissa. Tietoturvavaatimusten laatimista on kuvattu kappaleessa ”**Tietoturvavaatimusten kuvaaminen**”.

Tietoturvariskejä listattiin järjestelmän normaalin ja poikkeavan toiminnan kannalta. Riskianalyysin pohjalta laadittiin uhka-analyysi. Tietoturvariskejä ja uhkia käsiteltiin erillisissä työpalavereissa. Riski- ja uhka-analyysin laatimista on kuvattu kappaleessa ”**Tietoturvariski- ja uhka-analyysin kuvaaminen**”.

Tietoturva-arkkitehtuuri perustui NM2-järjestelmän teknisiin kuvauksiin sekä tietoturvavaatimuksiin siitä, miten palvelun käyttö ja toiminnallisuus on ratkaistu loppukäyttäjän kannalta tietoturvallisesti. Tietoturva-arkkitehtuurin laatiminen on kuvattu kappaleessa ”**Tietoturva-arkkitehtuurin kuvaaminen**”.

Testaus- ja auditointisuunnitelma perustui kehityksen alla olevan palvelun systeemitason testausperiaatteisiin. Tässä suunnittelussa hyödynnettiin käyttötapausten yhteydessä listattuja poikkeustilanteita ja tietoturvariskianalyysin tuloksia testaustapauksia laadittaessa. Testaus- ja auditointisuunnittelun laatimista on kuvattu kappaleessa ”**Testaus- ja auditointisuunnittelu**”.

Palvelulle määriteltiin realistiset tietoturvatavoitteet palvelukuvausten ja tietoturva-vaatimusten ja -analyysien pohjalta. Tietoturvatavoitteet vastuutettiin palvelun tuotantoketjun osapuolten kesken. Tietoturvatavoitteiden laatimista on kuvattu kappaleessa ”**Tietoturvatavoitteiden kuvaaminen**”.

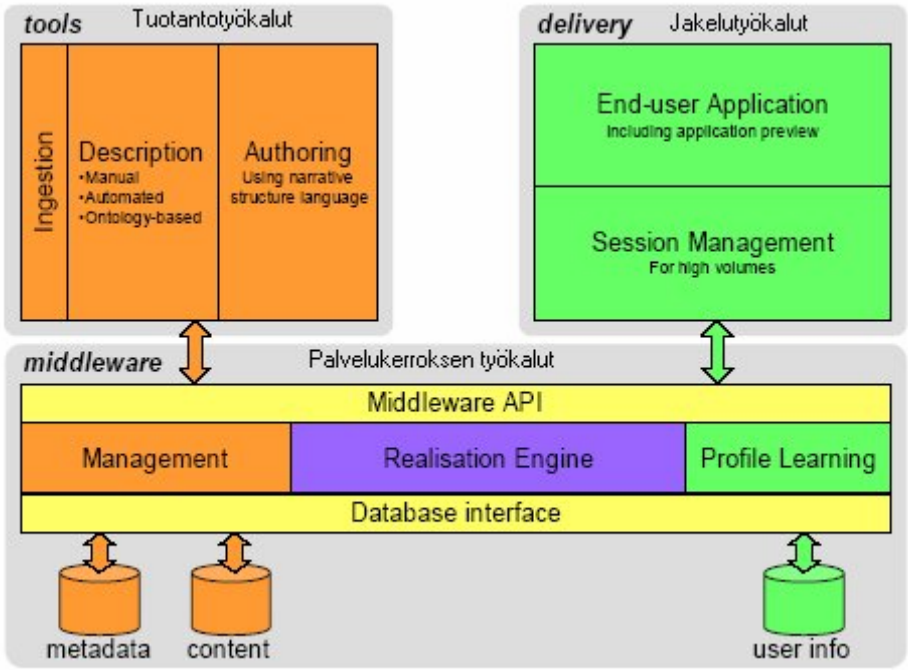
2. New Media, New Millenium (NM2) -järjestelmä

NM2-projektissa luodaan mediateollisuudelle järjestelmätyökaluja, joita voidaan käyttää erilaisten liikkuvaa kuvaa hyödyntävien mediatuotantojen kehityksessä ja jakelussa laajakaistaverkoissa. NM2-järjestelmän työkalujen kehityksessä on huomioitu kaikkien seitsemän eri NM2-projektiin kuuluvan mediatuotannon vaatimukset. Järjestelmä-työkalut voidaan jakaa tuotanto- ja jakelutyökaluihin sekä näitä työkaluja yhdistävän palvelukerroksen (middleware) työkaluihin (kuva 3).

Tuotantotyökalut liittyvät olemassa olevan media-aineiston tallentamiseen NM2-järjestelmän käyttöön, mediaelementtien tunnistamiseen ja kuvaamiseen metatiedoilla sekä työkaluihin, joilla kuvataan tarinankerronnallisia sisältörakenteita ja liitetään niihin sääntöjä siitä, miten ja mitä mediaelementtejä tällaiseen rakenteeseen voidaan liittää.

Palvelukerroksen työkalut liittyvät tuotantoon ja jakeluun. Pääsääntöisesti palvelukerros vastaa digitaalisen median ja näihin liittyvän metadatan sekä käyttäjien profiilitiedon hallinnasta. Palvelukerros vastaa myös käyttäjälähtöisen ja interaktiivisen median reaaliaikaisesta koostamisesta jakelua varten.

Jakelutyökalut liittyvät palvelukerroksessa koostetun median jakeluun ja kommunikointiin käyttäjien kesken. Jakelukerroksen vaatimukset ja ratkaisut NM2-projektiin kuuluville seitsemälle eri mediatuotannolle ovat erilaiset.

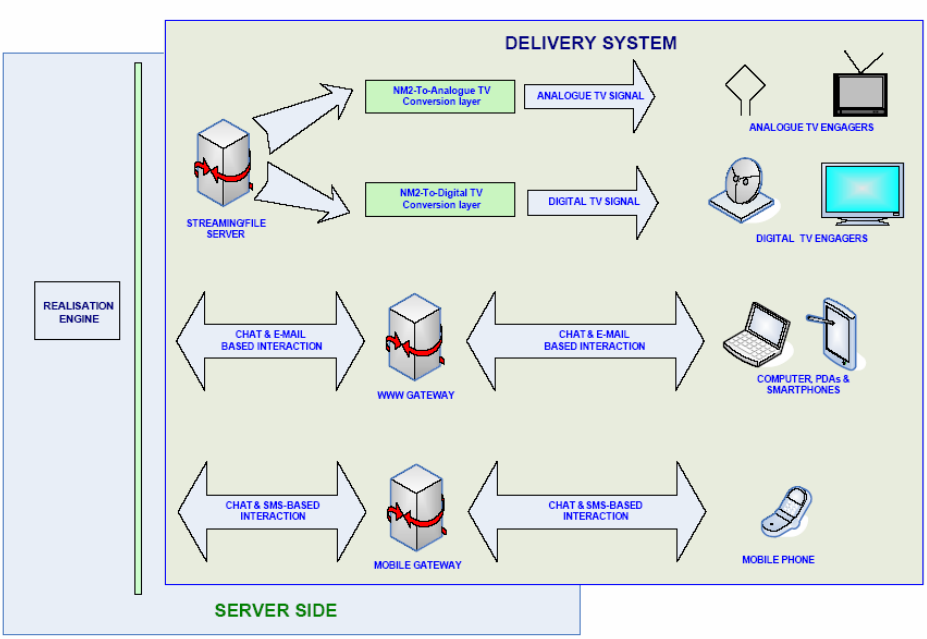


Kuva 3. NM2-järjestelmä muodostuu mediatuotantoon ja -jakeluun tarkoitetuista työkaluista [3].

2.1. NM2-järjestelmän käyttö Vahinkolaukauksia-tuotannossa

NM2-projektin tuloksia hyödynnetään Vahinkolaukauksia-tuotannossa siten, että Vahinkolaukauksia-käsikirjoituksen mukainen rakenne kuvataan tuotantotyökalulla rakenteeksi, joka kuvaa tarinan eri etenemisvaihtoehdot ja säännöt, millä ehdoilla eri mediaelementit voivat liittyä tarinan eri kohtiin.

NM2-järjestelmään rakennetaan rajapinta, joka vastaanottaa ja lähettää tekstiviestejä. Saapuneet tekstiviestit käsitellään järjestelmän loppukäyttäjätyökalulla, jota operoi moderaattori. Järjestelmään saapuneet tekstiviestit vaikuttavat yhdessä moderaattorin vaikutuksella siihen, miten realisointikone täydentää dynaamisesti tarinarakenteen. Realisointikone hakee mediaelementit tietokannasta ja muodostaa ns. soittolistan (mediavirran) video- ja audiomediaelementeistä. Jakelujärjestelmä vastaa muodostetun soittolistan konvertoimisesta TV-lähetykseen soveltuvaksi signaaliksi (kuva 4).



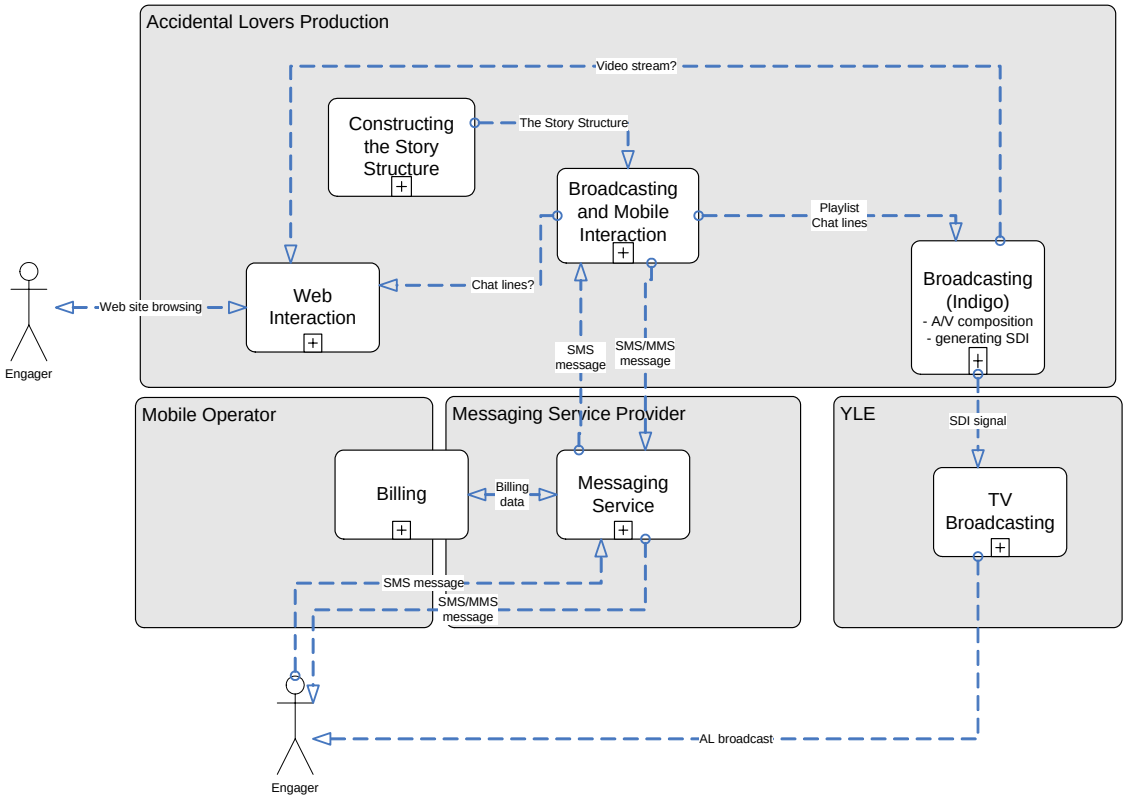
Kuva 4. Jakelujärjestelmä tarjoaa useita eri kanavia NM2-järjestelmään [3].

3. Tietoturvan huomioiminen Vahinkolaukauksia-hankkeessa

3.1. Palveluprosessin ja käyttötapausten kuvaaminen

Tietoturvavaatimusten löytämiseksi projektissa kuvattiin Vahinkolaukauksia-konseptin palveluprosessit. Prosessit kuvattiin BPMN-notaatiolla niiltä osin kuin ne liittyivät itse rakennettavaan konseptiin. Ulkoiset prosessit jätettiin kuvaamatta, vain liittymät ulkoisin prosesseihin kuvattiin.

Prosessikokonaisuudesta laadittiin prosessikartta, jonka pohjalta tehtiin päätökset tarkemmin kuvattavista prosesseista. Tietoturvan kannalta keskeiseksi prosessiksi osoittautui ”Broadcasting and Mobile Interaction” -prosessi, johon tuotannon keskeinen toiminnallisuus sisältyy.

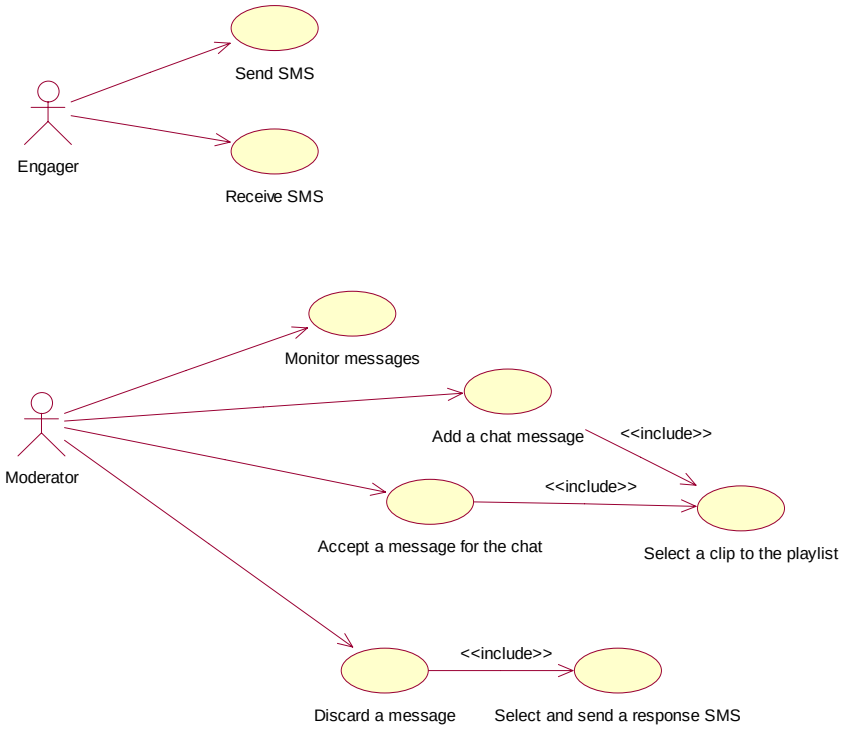


Kuva 5. Prosessikartta Vahinkolaukauksia-hankkeeseen liittyvistä prosesseista.

Prosessikaaviot toimivat lähtökohtina käyttötapausmallinnukselle. Käyttötapausmalli muodostettiin UML-notaation mukaisesti. Käyttötapausmalli sisältää graafiset kuvaukset, käyttötapauskaaviot, kunkin käyttötapauksen sanallisen kuvauksen sekä kuvaukset järjestelmän aktoreista. Käyttötapausmallissa kuvataan käyttäjien ja järjestelmän välinen interaktio, keskeiset käsittelysäännöt sekä varsinkin tietoturva-vaatimusten kannalta olennaiset, kunkin käyttötapauksen yhteydessä mahdolliset

poikkeustilanteet. Käyttötapausten tekstikuvauksissa käytettiin TietoEnatorin ohjelmistotuotantoprosessin mukaista oletuslomakepohjaa, jonka avulla voitiin selkeästi erotella kunkin käyttötapauksen normaalitilanteen mukainen toiminnallisuus mahdollisista poikkeustilanteista.

Käyttötapausmallin laatiminen kohdistui tietoturvan kannalta keskeisiin käyttötapauksiin. Käytännössä tämä tarkoitti ”Broadcasting and Mobile Interaction” -prosessin toiminnallisuuden sisältämiä käyttötapauksia. Prosessikuvauksen perusteella etsittiin alustavat käyttötapaukset, joita iteratiivisesti työstämällä muodostettiin lopullinen käyttötapausmalli.



Kuva 6. Käyttötapauskaavio ”Broadcasting and Mobile Interaction”.

Huomioita prosessi- ja käyttötapausmallinnuksesta

Sen lisäksi, että käyttötapauskuvausten perusteella muodostettiin tietoturva-vaatimuksia, käyttötapausmalli toimi apuna sekä Vahinkolaukauksia-konseptin että siihen liittyvien uusien ohjelmistotuotteiden toiminnallisuuden määrittelyssä.

Tietoturvan mallinnuksen kannalta on oleellista, että prosessi- sekä käyttötapaus-kuvauksia laadittaessa on mukana tietoturva-asiantuntija, joka voi analysoida käyttötapauksia mahdollisten poikkeavien toimintojen kannalta. Tässä vaiheessa tunnistetut tietoturvaa koskevat havainnot voidaan hyvin ottaa huomioon vielä sovelluskehityksessä.

3.2. Tietoturvavaatimusten kuvaaminen

Vahinkolaukauksia-hankkeessa alustavat tietoturvavaatimukset johdettiin laadituista prosessi- ja käyttötapauskaavioista sekä NM2-järjestelmäkehitykselle aikaisemmin asetetuista toiminnallisista ja liiketoiminnan vaatimuksista. Näitä vaatimuksia käytiin läpi ja täydennettiin yhteisessä työpalaverissa. Samalla kirjattiin mahdollisia ratkaisuvaihtoehtoja.

Kaikki tietoturvavaatimukset luokiteltiin toiminnallisiin, lainsäädännöllisiin tai informaatiokohtaisiin vaatimuksiin sekä tämän lisäksi luokiteltiin näitä tarkentaviin alaluokkiin, kuten palvelun saatavuus, käytettävyys ja luottamuksellisuus. Jokainen vaatimus myös tyypitettiin sen mukaan, oliko se tekninen, hallinnollinen vai fyysinen. Vaatimus kuvattiin selkeästi ja arvioitiin lopuksi, otetaanko se mukaan toteutettavaksi sekä määriteltiin myös vastuutaho.

Tietoturvavaatimukset käytiin tietoturva-asiantuntijapalvelun ja palvelun tuottajan kanssa läpi työpalavereissa sekä toimitettiin järjestelmän toteuttajalle tehtäväksi. Järjestelmän toteuttaja lisäsi ratkaisun kunkin vaatimuksen kohdalle.

Keskeisimmät tietoturvavaatimukset liittyivät Vahinkolaukauksia-hankkeessa seuraaviin asioihin:

- Palvelun saatavuuteen, joka samalla liittyy katsojan saamaan käyttäjäkokemukseen. Esimerkiksi miten ohjelman katsoja reagoi siihen, jos hän ei saa luvattua paluuviestiä tai miten käyttäjää tiedotetaan, jos palvelu ei ole ollenkaan käytettävissä, jos järjestelmä ylikuormittuu.
- Palvelun suorituskykyyn, joka samalla liittyy palvelun laatuun ja käyttöön pidemmällä aikajänteellä. Esimerkiksi, jos katsoja ei saa tekstiviestiään ajoissa järjestelmään, jolloin hän ei pääse vaikuttamaan ohjelman kulkuun.
- Palvelun tuottamaan sisältöön siinä mielessä, mitä tekstiviestejä sisältönsä puolesta ei saa välittää ohjelmaan.
- Palvelun laskutuksen toimivuuteen siinä mielessä, että laskutusperusteet voidaan jälkikäteen todeta.

Huomioita tietoturvavaatimusten kuvaamisesta

Oleellista vaatimusmäärittelyn toteuttamisessa oli se, ettei NM2-projektissa erillisiä tietoturvatavoitteita oltu aikaisemmin huomioitu, joten tavoitetaso tietoturvan toteutuksen kannalta määräytyi vasta vaatimusmäärittelyn aikana. Laaditut tietoturva-vaatimukset pitää käydä läpi myös liiketoiminnan kanssa, jos niitä ei heiltä ole alun perin saatu tai eivät ole osanneet niitä kuvata oikein.

Tietoturvan mallinnuksen kannalta on oleellista, että tietoturvavaatimuksia laadittaessa on mukana myös tekninen arkkitehti, joka tuntee järjestelmän ja ympäristön, jossa sitä tullaan käyttämään, jotta myös järjestelmätason tietoturvaratkaisut voidaan huomioida sovelluskehityksessä. Lainsäädäntöön viittaavissa vaatimuksissa olisi oltava myös lakiasiaintuntemusta käytettävissä.

Toteutuksen kannalta on oleellista, että tietoturvavaatimusten, kuten muidenkin vaatimusten, toteutumista seurataan.

3.3. Tietoturvariski- ja uhka-analyysin kuvaaminen

Vahinkolaukauksia-hankkeessa tietoturvariski- ja uhka-analyysi toteutettiin laadittujen tietoturvavaatimusten pohjalta. Tietoturvavaatimuksista tunnistettiin ne vaatimukset, joihin liittyi tietoturvariski, joka toteutuessaan vaikuttaisi palveluun.

Tietoturvariskit ja niihin liittyvät tietoturvavaatimukset listattiin. Jokaisen riskin osalta arvioitiin seurausaste sekä todennäköisyys sille, että riski toteutuu. Jotta riskiin osattaisiin varautua oikein, kuvattiin myös riskin toteutuessa pahin mahdollinen seuraamus palvelun kannalta sekä syy riskin toteutumiseen. Riskinhallintaa varten kuvattiin ennakoivat toimenpiteet, joilla riskin vaikutusta voidaan lieventää tai estää kokonaan riskin toteutuminen. Riskienhallinnan kannalta nimettiin myös vastuutaho.

Prioriteetiltaan suurimmat riskit kohdistuivat ulkopuolisiin osapuoliin, joiden palveluja mm. tietoliikenneresursseja Vahinkolaukauksia-tuotanto hyödyntää. Näiden riskien eliminoimiseksi palvelusopimukset osoittautuivat ainoaksi ratkaisuksi.

Tietoturvariski- ja uhka-analyysi toteutettiin samalla kokoonpanolla kuin tietoturva-vaatimusmäärittelyt ts. tietoturva-asiantuntijapalvelun ja palvelun tuottajan kanssa käytiin läpi työpalavereissa sekä toimitettiin järjestelmän toteuttajalle kommentoitavaksi. Vahinkolaukauksia-hankkeessa ei riskikartoitettu järjestelmä-suunnittelua, mikä olisi edellyttänyt enemmän aikaa, erityisosaamista ja perehtyneisyyttä mediatuotannon järjestelmiin. Toisaalta järjestelmäkehitys oli jo toteutusvaiheessa niin pitkällä, että aikaisempaan suunnitteluun ei enää tässä vaiheessa kannattanut puuttua. Todettiin, että tämä tulee huomioida järjestelmätestauksen suunnittelussa.

Keskeisimmät tietoturvariskit liittyivät Vahinkolaukauksia-hankkeessa seuraaviin asioihin:

- Palvelun kuormitukseen, joka samalla liittyy palvelun saatavuuteen. Tässä huomioitiin myös vastakkainen reaktio eli jos katsojat eivät lähetä riittävästi tekstiviestejä ohjelmaan. Keskeisenä seikkana tässä on järjestelmän laajennettavuus ja toiminnallisuus, joka ottaa huomioon suuret tekstiviestimassat sekä vähäiset tekstiviestimäärät.
- Palvelun sisältöön, esimerkiksi järjestelmä tuottaa vastaanottamistaan teksti-viesteistä aina samansisältöisen tarinan. Keskeisenä seikkana tässä on tunnistaa tekstiviestimassasta mahdollinen epäystävällinen hyökkäys palvelua kohtaan.

- Palvelun eheyteen, häiriöttömyyteen ja laatuun, jotka samalla liittyy käyttäjäkokemukseen joko positiivisesti tai negatiivisesti. Keskeisenä seikkana tässä on tunnistaa ympäristötekijät, jotka voivat vaikuttaa palveluun, esimerkiksi operaattoripalvelut, tietoliikenneyhteydet ja fyysisen tietoturvan toteutus.

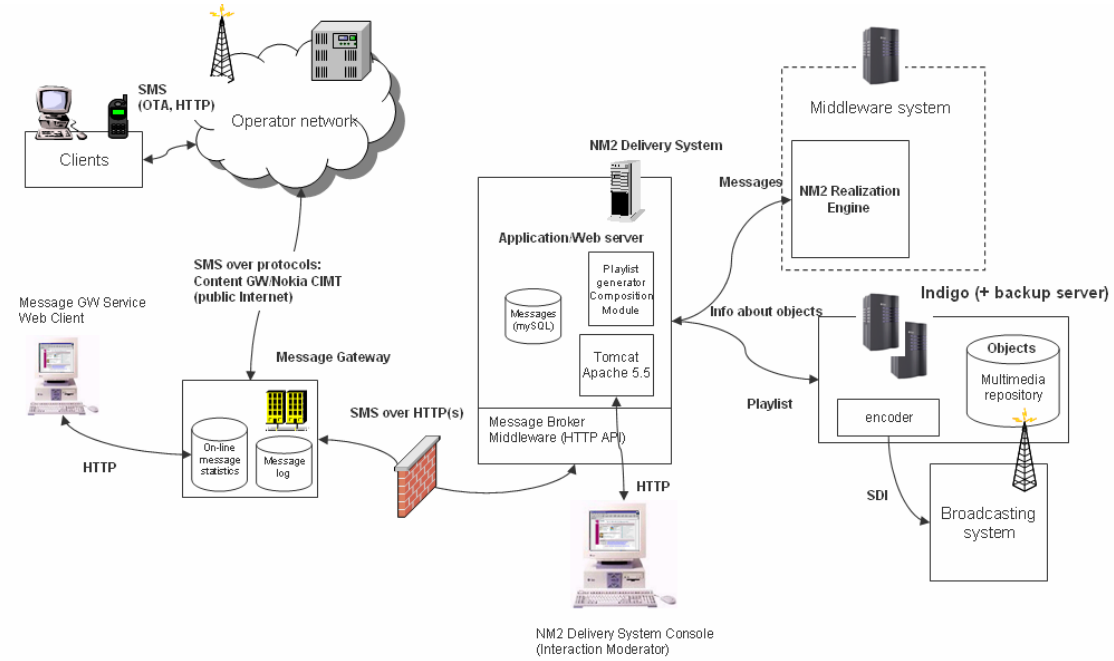
Huomioita tietoturvariskien kuvaamisesta

Tietoturvariskien tunnistukseen pitää osallistua henkilöitä, joilla on kehitettävän järjestelmän lisäksi asiantuntemusta ympäristöstä, jossa järjestelmää käytetään tai joihin se liittyy, mm. kolmannen osapuolen järjestelmät. Vahinkolaukauksia-hankkeessa tällaista asiantuntemusta edellytetään mm. mobiili- ja operaattori-ympäristöistä.

Useimmiten riskien eliminoimiseen kuvatut toimenpiteet ovat järjestelmäkehitykseen ja palvelun tarjontaan nähden kalliita, jolloin pitäisi harkita sellaisia toimenpiteitä, joilla riskin todennäköisyys saadaan pienemmäksi, mutta ei täysin eliminoitua. Useimmiten tällöin ratkaisu on kustannuksiltaan hyväksyttävissä.

3.4. Tietoturva-arkkitehtuurin kuvaaminen

Vahinkolaukauksia-hankkeessa tietoturva-arkkitehtuurin kuvaus toteutettiin NM2-järjestelmäkuvauksiin ja esitettyyn tavoitetilan liiketoimintamalliin pohjautuen. Lisäksi selvitettiin tekstiviestivälityspalveluja tarjoavat yritykset ja valittiin Vahinkolaukauksia-hankkeeseen kriteerit täyttävä, välityspalveluja tarjoava operaattori, jonka tarjoaman järjestelmän API-rajapintakuvausten avulla toteutettiin liityntä NM2-järjestelmään, jotta tekstiviestit pystyttiin vastaanottamaan ja paluuviestit pystyttiin lähettämään katsojille takaisin. Tässä kartoituksessa pyrittiin varmistamaan viestinvälitysoperaattorin palvelun taso mm. suorituskyky ja laskutuksen toteutus. Vahinkolaukauksia-tuotannon toteuttava tietoturva-arkkitehtuuri kuvattiin lähinnä loogisesta näkökulmasta. Se kuvaa palveluun kuuluvat järjestelmät ja niiden väliset riippuvuudet. Tietoliikenteen osalta erillistä kuvausta ei tehty, koska ainoat liitynnät NM2-järjestelmästä ulospäin on yhteys viestinvälitysoperaattorille ja kiinteä yhteys YLElle televisiosignaalin jakelua varten (kuva 7).



Kuva 7. NM2-järjestelmän looginen arkkitehtuuri Vahinkolaukauksia-tuotannossa.

Huomioita tietoturva-arkkitehtuurin kuvaamisessa

Tietoturva-arkkitehtuurin suunnittelussa otettiin huomioon mm. seuraavat liiketoiminnan reunaehdot toteutettavalle järjestelmälle:

- Järjestelmän pitää pystyä vastaanottamaan ja käsittelemään 40 000 tekstiviestiä tunnissa. Tämä edellyttää operaattoreilta järjestelyjä, joilla taataan viestinvälitys-palvelun toimivuus ruuhka-aikoina ja NM2-järjestelmältä kuormitettavuutta. Tekstiviestien viiveet on myös minimoitava, ja tilanteissa, joissa viestiä ei voida vastaanottaa operaattorin sanomaviestinkeskukseen, on viestin lähettäjää informoitava verkon ruuhkautuneisuudesta.
- Tekstiviestin viive katsojalta siihen, kun se ilmestyy ohjelmaan TV-ruudulle, ei tulisi olla muutamia sekunteja pidempi. Tässä ei huomioida moderaattorin käyttämää aikaa tekstiviestien käsittelyyn eikä realisointikoneen, Indigo-koneen ja YLEn järjestelmien aiheuttamaa viivettä.
- Jos realisointikoneen yhteys Indigo-järjestelmään katkeaa, SDI-signaalin tuottaminen ei katkea. Käytännössä tämä tarkoittaa sitä, että ohjelma etenee Indigo-järjestelmään etukäteen tallennetun tarinan mukaan.
- Jos Indigo-järjestelmä kaatuu, saadaan se 10 minuutissa takaisin toimintaan ja lähetys jatkuu siitä kohdasta, mihin se jäi ennen kaatumista.

3.5. Testaus- ja auditointisuunnittelu

Vahinkolaukauksia-hankkeessa testaus- ja auditointisuunnittelu pohjautui testaussuunnitelmaan, jonka tarkoituksena oli katselmoida, että toteutettu järjestelmä täyttää siltä odotetut vaatimukset sekä tuotantoympäristö täyttää hallinnolliset rutiinit ja fyysinen suojaus täyttää tietoturvavaatimukset. Testaussuunnittelu tehtiin yhteistyössä NM2-osapuolten ja LUOTI-hankkeen kesken.

Testaussuunnitelmassa kuvattiin myös systeemitestauksen testitapaukset. Testitapauksiin kuvattiin myös järjestelmältä odotettu käyttäytyminen eli miten järjestelmä jatkaa esim. häiriötilanteissa toimintaansa. Systeemitestauksen lisäksi sovittiin erillisestä käytettävyystestistä, yleisötestistä sekä tietoliikennetestistä.

Testitapaukset jaettiin neljään kategoriaan:

- Testitapauksiin, joilla testataan ja mitataan järjestelmän normaalia (suunniteltua) käyttäytymistä.
- Testitapauksiin, joilla testataan ympäristön aiheuttamia häiriö- ja kuormitustilanteita.
- Testitapauksiin, joilla testataan käyttäjän ennalta arvaamatonta käyttäytymistä.
- Testitapauksiin, joilla testataan, onko järjestelmä suunniteltu tietoturvallisesti eli löytyykö järjestelmästä tietoturva-aukkoja.

Testaus- ja auditointisuunnittelu perustui käyttötapauksiin, tietoturvariskianalyysin tuloksiin, tunnettuihin tietoturva-aukkoihin ja järjestelmän resurssien kuormitettavuuteen.

Huomioita testaus- ja auditointisuunnittelusta

Yleensä testauksen- ja auditoinnin yhteydessä tai ennen niitä toteutetaan katselmointi, jolla varmistetaan, että toteutettu järjestelmä täyttää siltä vaaditut tietoturva-vaatimukset. Katselmointi tehdään tietoturvavaatimusten, järjestelmäkuvausten, suunnittelun ja toteutuksen kuvausten sekä tietysti testaussuunnitelman pohjalta. Vahinkolaukauksia-hankkeessa ei katselmointia tehty, koska tiedettiin, että tietoturva oli jätetty tietoisesti huomioimatta järjestelmän suunnittelun aikana. Toisaalta järjestelmän suunnittelun ja toteutuksen syvällisempään katselmointiin ei ollut resursseja ja aikaa. Tämä olisi edellyttänyt NM2-projektilta seuraavia nimikkeitä, joista monet olivat jo olemassa:

- järjestelmäkuvaukset sisältäen laitteisto-, ohjelmisto- sekä järjestelmän liityntäkuvaukset
- suunnitteluaineisto sisältäen arkkitehtuuri- ja suunnittelukuvaukset, toiminnalliset kuvaukset, yksityiskohtainen suunnittelu sekä ohjelmakoodi mahdollista koodin katselmointia varten

Katselmointi, auditointi ja testaus pitäisi teettää ulkopuolisella asiantuntijalla, jotta näkemys järjestelmän tilanteesta voidaan laatia ilman mitään sidonnaisuuksia ja puolueettomasti.

3.6. Tietoturvatavoitteiden kuvaaminen

Vahinkolaukauksia-hankkeessa tietoturvatavoitteet johdettiin NM2-järjestelmän määrittelyistä: NM2-järjestelmäkuvauksista, tuotanto-, prosessi-, käyttötapaus- ja arkkitehtuurikuvauksista, tietoturvavaatimuksista sekä riskianalyysin tuloksista. Työpalaverit Vahinkolaukauksia-tuotannon osapuolten kanssa muodostivat kuvan kehitettävän järjestelmän tietoturvatavoitteista.

Osana tietoturvatavoitteita seuraavat periaatteet toteutuksen ja suunnittelun osalta todettiin NM2-järjestelmäkehityksen kannalta merkittäviksi:

- Sovelluksen kuormitettavuus: varmista, että sovellus toimii oikein tilanteissa, joissa järjestelmää kuormitetaan suurilla määrillä tekstiviestejä.
- Sovelluksen käytettävyys: varmista, että sovelluksen käyttö on looginen ja käyttäjän toimintoja ja loogisia valintoja tukeva. Tässä tarkoitetaan moderaattorin työkalua, jolla tekstiviestejä käsitellään.
- Sovelluksen haavoittuvuuksien tiedostaminen: varmista, että järjestelmässä käytettyjen valmisohjelmistojen ja käyttöjärjestelmien tunnetut tietoturva-aukot on korjattu. NM2-järjestelmä on pääosin tuotettu NM2 EU-projektissa, mutta esimerkiksi järjestelmään liitettävät median käsittelyohjelmistot/-järjestelmät, kuten Indigo, ovat kolmannen osapuolen järjestelmiä, jotka saatiin Vahinkolaukauksia-hankkeen käyttöön.
- Järjestelmän konfigurointi on tehty oikein: varmista, että NM2-järjestelmä on konfiguroitu oikein esim. tekstiviestirajapinnassa käytetty web-palvelin ei sisällä tietoturva-aukkoja.
- Järjestelmän pääsynvalvonta ja ylläpito on rajoitettu: varmista, että järjestelmään pääsee tarkoin määritellyistä rajapinnoista, ja järjestelmän ylläpitorajapinnat on kuvattu. Tällä tarkoitetaan niin NM2-järjestelmän omien sovellusten, kuten moderaattorin työkalun (Interaction Moderation), realisointikoneen (Realization Engine) että tekstiviestien välityskomponentin ja operaattoripalveluja tarjoavan tahon järjestelmien suojaamista oikein.
- Salauksen käyttö: varmista, että käytettävän suojauksen taso on riittävä ja salausta on käytetty oikein.

Huomioita tietoturvatavoitteiden kuvaamisesta

Tietoturvatavoitteiden kuvaamisessa oleellista on käydä tunnistetut tietoturva-vaatimukset läpi ja arvioida ne uudestaan siltä kannalta, miten ymmärrettäviä, yksiselitteisiä ja vertailtavia ne ovat. Mikään vaatimus ei saa sulkea pois toista vaatimusta tai olla ristiriidassa toisen vaatimuksen kanssa. Jos näin kuitenkin tapahtuu, on vaatimukset priorisoitava sen mukaan, mikä pitää toteuttaa ensisijaisesti ja mikä toissijaisesti.

Tietoturvatavoitteiden kuvaamisessa oleellista on tunnistaa vaatimuksen alkuperä ja osoittaa vaatimukselle omistaja, jotta tarvittaessa vaatimuksen tarkoitusta voidaan täsmentää. Tietoturvatavoitteet, siinä missä muut vaatimukset, tekniset tai liiketoimintavaatimukset, pitää kuljettaa ohjelmistokehitysprosessin läpi, jotta vaatimusten alkuperä ja jäljitettävyys voidaan tarvittaessa osoittaa.

Tietoturvatavoitteet pitää katselmoida, sillä niiden perusteella tehdään päätös jatketaanko järjestelmäkehitystä kuvatulla tietoturvatasolla. Katselmoinnissa pitää olla mukana asiantuntijoita, joilla on tietämystä tietoturva-asioista, järjestelmäympäristöstä ja järjestelmän käyttötarkoituksesta.

3.7. Merkittävimmät esille tulleet tietoturvakysymykset

Vahinkolaukauksia-hankkeen aikana merkittävimmiksi tietoturva-aiheiksi osoittautuivat palvelun saatavuus, palvelun looginen toimivuus, käyttäjäkokemus, järjestelmän toimintavarmuus, järjestelmän haavoittuvuus ja fyysinen tietoturva. Näitä keskeisimpiä aiheita on käsitelty alla olevassa taulukossa millään tavoin niitä priorisoimatta.

Taulukko 1. Vahinkolaukauksia-hankkeessa esille tulleet tietoturvakysymykset.

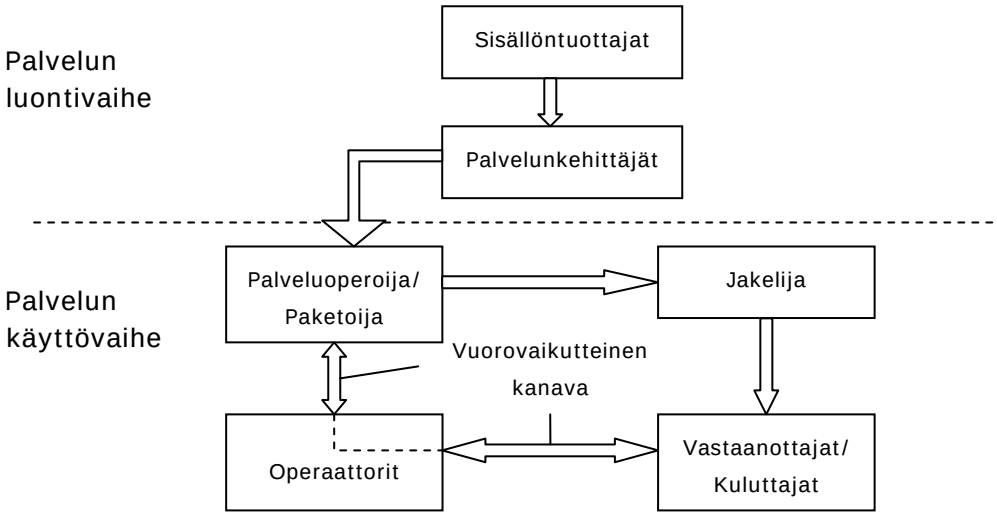
	Riski	**Ongelma ja ratkaisuehdotus**
Palvelun saatavuus	Katsoja ei saa lähettämälleen tekstiviestille paluuviestiä tai saa sen liian myöhään. Tällöin katsojan motivaatio lähettää useampia tekstiviestejä vähenee.	Ongelma voi johtua verkkoviiveistä tai järjestelmän kuormituksesta. Tällöin verkon kuormitustasoa pitää seurata ja ongelmatilanteissa tiedotetaan katsojaa lähetyksessä tekstiviestien käsittelyssä tapahtuvasta viiveestä.
Palvelun looginen toimivuus	NM2-järjestelmään ei saada riittävästi tekstiviestejä ohjelman tarpeisiin nähden.	Ongelma voi johtua siitä, että mobiiliverkko on kuormittunut tai tekstiviestivälityspalvelu monioperaattoriympäristössä ei toimi oikein. Tällöin NM2-järjestelmässä moderaattorin pitää tuottaa sanomia tai käyttää järjestelmään etukäteen tallennettuja sanomia, jotka sopivat näytöksen kohtiin. Ongelma tiedotetaan katsojille lähetyksessä.
Käyttäjäkokemus	Sama juoni toistuu eri lähetyskerroilla, jolloin se ei houkuttele uusia katsojia ja vanhat katsojat lopettavat ohjelman katsomisen.	Ongelma voi johtua siitä, että katsojat lähettävät samankaltaisia tekstiviestejä, jolloin avainsanatunnistus tuottaa aina saman tuloksen. Tällöin NM2-järjestelmän täytyy pitää kirjaa aikaisemmin valituista mediaobjekteista, jottei niitä tulisi liian usein valittua ja näytökset vaihtelevat eri lähetyskerroilla. Myös moderaattori voi vaikuttaa, mitä viestejä näytetään lähetyksessä.
Palvelun looginen toimivuus	Vastaanotettuja tekstiviestejä ei pystytä käsittelemään ajoissa, jolloin kaikki vastaanotetut tekstiviestit eivät pysty vaikuttamaan ohjelman kulkuun tai järjestelmä käsittelee tekstiviestejä, jotka eivät ole synkronissa lähetyksen kanssa eikä avainsanatunnistus tuota relevantteja tuloksia.	Ongelma johtuu siitä, että suuri joukko tekstiviestejä odottelee käsittelyvuoroa. Ratkaisuna voidaan NM2-järjestelmän prosessointikapasiteettia kasvattaa tai vastaanotettuja tekstiviestejä ei käsitellä siinä järjestyksessä, kun ne saapuvat vaan käsittelyvuoroon poimitaan lähinnä viimeksi lähetetyt tekstiviestit.

	Riski	Ongelma ja ratkaisuehdotus
Järjestelmän toimintavarmuus	Verkkoyhteydessä NM2-järjestelmän ja YLEn lähetysjärjestelmän välillä on häiriöitä, jolloin ohjelmaa ei voida lähettää tai lähetyksessä ilmenee ongelmia.	Ongelma voi johtua NM2-järjestelmän lähiverkosta tai kaapeliyhteydestä YLEn toimitiloihin. Ratkaisuna nähdään tietoliikenneyhteyden toimivuuden varmistaminen vaihtoehtoisella yhteydellä esim. reitityksen avulla. Tietoliikenneyhteyttä (signaalin tasoa) pitäisi seurata reaaliajassa (esim. kapasiteettia). Toisena vaihtoehtona voidaan lähettää etukäteen nauhoitettua versiota ohjelmasta tai viimeisenä vaihtoehtona muun ohjelman lähettämistä.
Järjestelmän toimintavarmuus	Operaattoriympäristössä on häiriöitä, minkä vuoksi NM2-järjestelmä ei saa katsojien lähettämiä tekstiviestejä tai katsojat eivät saa paluuviestejä.	Ongelma voi johtua operaattoriympäristön toimintahäiriöistä tai ylikuormittumisesta. Tällaisissa tapauksissa moderaattorin täytyy tuottaa tekstiviestejä tai hyödyntää järjestelmään etukäteen tallennettuja viestejä.
Järjestelmän toimintavarmuus	Tuotantojärjestelmän laitteistoresurssi (esim. levy) rikkoontuu.	Ongelma on useimmiten ennalta arvaamaton ja toteutuu yllättäen. Ratkaisuna nähdään kahdennettujen laitteistoresurssien käyttö kriittisten komponenttien osalta (esim. kahdennettu levy).
Järjestelmän haavoittuvuus	Tuotantoympäristö joutuu tietoturvahyökkäysten kohteeksi tai ympäristöön pääsee virus, joka aiheuttaa järjestelmän epätoivottua käyttäytymistä. Yhteydet tekstiviestivälityspalveluja tarjoavan operaattoritahon ja NM2-järjestelmän välillä ovat poikki tietoturvahyökkäyksen vuoksi. Hyökkäys ei välttämättä kohdistu suoraan kumpaakaan kohteeseen, mutta Internet-yhteys on poikki.	Ongelma johtuu tuotantoympäristön heikosta suojautumisesta ja varautumisesta tietoturhauhkiin. Tietoturvauhkia on monia, mutta useimpiin voidaan varautua. Esimerkiksi asiaton pääsy tuotantoympäristöön estetään ja liikennettä kontrolloidaan, virustorjuntapäivitykset pidetään ajan tasalla ja ainoastaan sallittu tietoliikenne tuotantoympäristöön hyväksytään sekä tietoa siirretään salatussa muodossa.
Järjestelmän toimintavarmuus	Operaattoriympäristön laskutus ei toimi oikein.	Ongelma johtuu laskutusjärjestelmän häiriöistä tai laskutusperusteiden puutteesta (tekstiviestejä ei laskuteta). Ratkaisuna laskutuksen tarkistukseen ja sitä kautta sen toiminnan seuraamiseksi nähdään transaktioiden seurantaa ja auditointia operaattoriympäristössä ja NM2-järjestelmässä, esim. tekstiviestiliikenteen osalta lokitiedon keräämistä.
Fyysinen tietoturva	Tuotantoympäristön fyysistä turvallisuutta ei ole toteutettu oikein (esim. pääsynvalvontaa ei ole toteutettu riittävällä tasolla, kiinteistössä tapahtuviin vikatilanteisiin ja niistä aiheutuviin uhkiin ei ole varauduttu, kuten vesivahinko tai tulipalo).	Ongelma johtuu puutteellisesta auditoinnista ja tuotantoympäristön katselmoinnista tuotantokäyttöön sopivaksi. Ongelmatilanteiden kartoittamiseksi fyysinen auditointi (kiinteistö- ja laitetilojen osalta) pitää toteuttaa ja riittävä valvonta tuotantoympäristöön pääsystä ja tuotantojärjestelmän resurssien käytöstä pitää toteuttaa.

4. Tietoturvan ratkaiseminen tuotantoketjussa

4.1. Palvelun tuotanto ja roolit

Vahinkolaukauksia-hankkeessa luotavan viihdepalvelun arvoverkkoon kuuluu useita eri osapuolia, joilla kullakin on oma roolinsa tietoturvan ratkaisemisessa (kuva 8). Arvoketjun osapuolet liittyvät joko palvelun luonti- tai käyttövaiheiseen. Samat osapuolet voivat toimia useassa roolissa.



Kuva 8. Vahinkolaukauksia-hankkeessa on useita arvoketjun osapuolia.

Sisällöntuottajina hankkeessa toimii Vahinkolaukauksia-tuotannon käsikirjoittaja, editoija, tuottaja, ohjaaja sekä monet ohjelmaformaatin luontiin osallistuvat henkilöt kuten näyttelijät. Kaikkiaan hankkeeseen osallistuu reilu 100 henkilöä. Palvelun kehittäjinä hankkeessa toimivat edellisten lisäksi teknologiayhteistyökumppanit NM2- ja LUOTI-projekteista. Palvelun käyttövaiheessa palvelun paketoijina toimivat NM2-järjestelmän operoijat, jotka tuottavat valmista ohjelmaa jakelijalle (tässä YLE). Katsojat toimivat palvelun kuluttajina, joilla on mahdollisuus vaikuttaa palvelun paketoimiseen lähettämällä tekstiviestejä TV-lähetykseen. Katsojat saavat vastikkeeksi paluuviestejä. Operaattorit toimivat viestiliikenteen välittäjinä ja maksuliikenteen hoitajana.

Palvelutuotantoketjun luonti- ja käyttövaiheisiin liittyy tietoturvavastuita, joista voidaan sopia sopimuksin. Edellä esitetyn arvoketjun osapuolten tietoturvavastuut voidaan pelkistää seuraavasti:

- Sisällöntuottajalla on vastuu tuottamastaan sisällöstä.
- Palvelun kehittäjällä on vastuu kehitetyn palvelun toimivuudesta ja laitetoimittajilla on vastuu palvelualustasta.

- Palveluoperoijalla on vastuu palvelun paketoinnista, jotta se vastaa sille asetettuja odotuksia niin laadullisesti kuin sisällöllisesti.
- Jakelijalla on vastuu palvelun häiriöttömästä jakelusta.
- Operaattoreilla on vastuu mobiiliviestiliikenteen välittämisestä ja laskutuksesta.

Lisäksi arvoketjun jakelijaan ja operaattoriin liittyy viranomaistaho, joilla on velvollisuus säädellä operaattoritoimintaa ja yleisverkkojakelutoimintaa.

Eri osapuolten rooli tietoturvan ratkaisemisessa koko kehitettävän palvelun näkökulmasta ei välttämättä tule esille, ellei jokin taho koordinoi koko palvelukehitys-prosessia ja osapuolet osallistu aktiivisesti palvelun kehittämiseen sen eri vaiheissa. Näin samalla varmistetaan, että eri osapuolten näkemykset ja vastuut tulevat myös todettua. Useimmiten tietoturva-asiat ovat hankalia ja järjestelmäkokonaisuudet niin isoja, ettei yksittäinen osapuoli pysty yksin sopimaan muiden puolesta käytetyistä tietoturvamenetelmistä, vaan näistä on sovittava yhteisesti.

Palvelukehitykseen voidaan tietoturvavaatimukset ottaa mukaan siinä missä muutkin vaatimukset. Yleisinä toimenpiteinä tietoturvaratkaisujen hakemiseksi ja toteuttamiseksi voidaan mainita:

- Varmistetaan, että tietoturva-asiat on huomioitu palvelukehityksessä.
- Määritellään järjestelmän tietoturvatavoitteet.
- Määritellään tietoturvavaatimukset järjestelmälle.
- Toteutetaan tietoturvavaatimukset ja parhaimmat käytännöt.
- Määritellään korjaustoimenpiteet haavoittuvuuksille.
- Määritellään tietoturvamittarit ja toteutetaan testaus.
- Julkaistaan toiminnalliset tietoturvaohjeet.
- Määritellään järjestelmän auditointikäytännöt.

5. Johtopäätökset

Vahinkolaukauksia-hanke valittiin LUOTI-ohjelmaan siinä vaiheessa, kun kehitettävän järjestelmän määrittelytyöt oli tehty. Suunnittelutyö Vahinkolaukauksia-tuotannon tarvitsemia työkaluja varten oli aloitettu ja toteutustyö muutaman työkalun osalta oli edennyt jo luonnosvaiheeseen. Huomioitavaa NM2-järjestelmän määrittelyvaiheesta oli, että tietoturvamäärittelyt oli jätetty tietoisesti pois. Siinä mielessä LUOTI-ohjelman tietoturva-asiantuntijapalvelulla ei pystytty vaikuttamaan järjestelmän määrittelyihin. Ainoastaan muutamiin suunnitteluvaiheessa oleviin tuotantotyökaluihin, asiantuntija-palvelussa pystyttiin esittämään toteutuksessa vielä huomioitavia tietoturvavaatimuksia. LUOTI-hanke antoi lisäarvoa NM2-kehityshankkeelle siinä mielessä, että sinällään itsestään selvinä pidetyt asiat jouduttiin käymään läpi tietoturvan näkökulmasta. Tällöin jouduttiin miettimään myös käytettävyyteen ja erilaisiin käyttötilanteisiin liittyviä poikkeustilanteita ja niihin reagoimista aivan eri näkökulmasta.

Järjestelmältä odotettavien toiminnallisten vaatimusten hahmottamiseksi järjestelmän käyttö ja siihen liittyvät oleelliset prosessit pitää kuvata. Näin saadaan selville mm. järjestelmän käyttöön ja palveluprosessiin liittyvät tietoturvavaatimukset. Vahinkolaukauksia-hankkeen tietoturvavaatimukset liittyivät usein järjestelmän käytettävyyteen, esim. miten vastaanotettuja tekstiviestejä olisi prosessoitava, jos niitä on paljon, jotta palvelun saatavuus ja käytettävyys taattaisiin riittävän hyvällä tasolla. Näin asiantuntijapalvelun tuottamat tietoturvavaatimukset toimitettiin NM2-projektin käyttöön.

Uhkakuvien ja riskien analysointi osoittautui hyväksi keinoksi hahmottaa mahdolliset ongelmatilanteet Vahinkolaukauksia-tuotannon järjestelmässä ja erityisesti sen käyttövaiheessa. Riskianalyysin päivittäminen järjestelmäkehityksen eri vaiheissa määrittelystä toteutukseen ja testauksesta käyttöönottoon kannattaa aina tehdä, sillä välttämättä hankkeen alkuvaiheessa ei pystytä hahmottamaan järjestelmän todellista käyttöä, esim. sen levinneisyyttä, käyttäjämääriä tai käyttäjien käyttäytymistä. Uhkakuvien hallinnalla pyritään varautumaan mahdollisiin ongelmatilanteisiin, minimoimaan vahinkoja uhkan toteutuessa tai jopa kokonaan poistamaan tai minimoimaan uhkakuva.

Vahinkolaukauksia-hankkeessa tietoturva liittyy pääsääntöisesti palvelun toimivuuteen ja sitä kautta sen saatavuuteen. Palvelun saatavuuteen vaikuttaa itse NM2-järjestelmän toteutuksen lisäksi kolmansien osapuolten järjestelmät, kuten operaattoripalvelut. Kolmansien osapuolten järjestelmien analysointi tietoturvan kannalta osoittautui epävarmaksi, koska se tehtiin haastatteluin eikä varsinaista auditointia ollut mahdollista tehdä. Siten tietoturvatestaus- ja auditointi tehdään ainoastaan NM2-järjestelmälle, jossa myös NM2-järjestelmän palvelin- ja verkkotietoturva sekä fyysinen tietoturva ovat keskeisiä asioita järjestelmää auditoitaessa. Vahinkolaukauksia-hankkeen NM2-järjestelmän auditointia ei ole tehty tämän raportin julkaisuhetkellä.

Vahinkolaukauksia-hankkeessa korostuivat seuraavat käytännöt ja niiden tärkeys palveluntuotantoketjussa:

- Tietoturvasuunnittelu on tehtävä muun järjestelmäsuunnittelun rinnalla eikä täysin erillisenä tehtävänä, sillä tietoturvamäärittelyt toimivat reunaehtoina muulle suunnittelulle, mm. käytettävyydelle ja informaation käsittelysäännöille. Palvelun kehityksen eri vaiheissa olisi verifioitava, miten alkuperäiset vaatimukset on huomioitu tai saavutettu.
- Liiketoiminta- tai palveluprosessien kuvaaminen ja tarkka suunnittelu on toimiva menettelytapa sekä liiketoimintalähtöisen tietojärjestelmäkehityksen että tietoturvasuunnittelun lähtökohtana. Liiketoiminnallisten vaatimusten pohjalta syntyviin tietojärjestelmävaatimuksiin on hyvä sisällyttää myös järjestelmälle asetettavat tietoturvavaatimukset.
- Yhteistyö ohjelmistokehittäjien ja tietoturva-asiantuntijoiden kanssa olisi hyvä aloittaa jo ohjelmistoprosessin alkuvaiheessa, mielellään jo vaatimusmäärittelyn yhteydessä.
- Koska palvelun tietoturvaan vaikuttaa palvelun arvoketjun kaikkien osapuolten tietoturvataso, olisi tietoturvavaatimukset käytävä jokaisen tahon kanssa läpi ja testattava toteutuksen taso koko arvoketjussa.
- Tietoturvan auditoinnin on oltava osa normaalia katselmusmenettelyä.
- Palvelun käyttökuormituksen arviointi voi olla aivan uudenlaisessa julkisessa palvelukonseptissa hankalaa, mikä asettaa omat haasteensa myös palvelun saatavuudelle asetettavien vaatimusten tarkalle määrittelylle.
- Tietoturva ja käytettävyys ovat sidoksissa toisiinsa ja useimmiten joudutaan tekemään kompromisseja toisen kustannuksella.

Lähdeviitteet

1. Marttila T., Saarinen L. and Nurminen M. 13.10.2005. Accidental Lovers Metadata Description. Document version 0.17. 14 pages.
2. Häikiö P., Saarinen L. and Tuomola M. 2004. Production-Description Part 7: Accidental Lovers. EC Report NM2 D2.3 – Public Deliverable. www.ist-nm2.org/.
3. NM2 partners. 15.3.2005. NM2 System Architecture, D2.4. NM2 deliverable (www.ist-nm2.org). 150 pages.