Sinikka Siironen

Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhat

Tietotekniikan kandidaatintutkielma

7. kesäkuuta 2016

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Sinikka Siironen

Yhteystiedot: sinikka.a.siironen@student.jyu.fi

Ohjaaja: Hannakaisa Isomäki

Työn nimi: Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhat

Title in English: Information security threats in software-defined networking

Työ: Kandidaatintutkielma

Sivumäärä: 24+2

Tiivistelmä: Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri on kehitetty nykyaikaisten tietoverkkojen, esimerkiksi pilvipalveluiden, tarpeisiin. Tässä tutkielmassa selvitettiin, mitä tietoturvauhkia ohjelmisto-ohjatussa tietoverkkoarkkitehtuurissa on, missä arkkitehtuurin osissa ne esiintyvät ja miten ohjelmisto-ohjatun tietoverkon ja perinteisen tietoverkon tietoturvauhat eroavat toisistaan. Tutkielmassa löydettiin tietoturvauhkia melko tasaisesti koko arkkitehtuurista, ja erityisesti hallintatason ja arkkitehtuurin tasojen rajapintojen tietoturvaa pidettiin tärkeänä. Kuitenkin ohjelmisto-ohjatun tietoverkon tietoturvaa tulee vielä tutkia kattavammin. Perinteiseen tietoverkkoon verrattuna ohjelmisto-ohjattu tietoverkko on turvallisempi, vaikka se aiheuttaakin uusia tietoturvaongelmia.

Avainsanat: ohjelmisto-ohjattu tietoverkko, tietoturva, tietoturvauhat

Abstract: Software-defined networking is an answer to the needs of the modern networks, such as cloud computing. This study attempts to survey the information security threats present in software-defined networking and their placement in the layers and interfaces of the architecture. Furthermore, the threats of the software-defined network are compared to the ones of a traditional network. In the study there were multiple information security threats found in the architecture, and they were spread across the architecture quite evenly. Especially the security of the control layer and the interfaces between layers was considered important. In conclusion, the security issues of software-defined networking still need to be studied more comprehensively. Compared to a traditional network, a software-defined network is more secure, even though it introduces new security threats.

Keywords: software-defined networking, information security, information security threats

Termiluettelo

Hallintakerros	Reititinarkkitehtuurin kerros. Engl. control plane.
Hallintataso	Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin keskimmäinen taso. Engl. control layer.
IETF	Internet Engineering Task Force. Internet-protokollia standardisoiva organisaatio.
OpenFlow	Ohjelmisto-ohjatun tietoverkon ohjaimen ja verkkolaitteen välinen viestintäprotokolla.
PKI	Public Key Infrastructure. TLS:ssä käytettävä julkisten avainten hallintajärjestelmä.
SDN	Software-Defined Networking. Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri.
SDN-sovellus	Ohjelmisto-ohjatun tietoverkon ohjaimen päällä ajettava sovellus.
Tiedonvälityskerros	Reititinarkkitehtuurin kerros. Engl. forwarding plane, data plane.
TLS	Transport Layer Security. Tietoliikenteen salausprotokolla.
Verkkoelementtitaso	Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin alin taso. Engl. infrastructure layer.
Verkkosovellustaso	Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin ylin taso. Engl. application layer.

Kuviot

Kuvio 1. Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin rakenne. 4

Taulukot

Taulukko 1. Kirjallisuuskartoitukseen valitut artikkelit. 8
Taulukko 2. Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhkia. 12
Taulukko 3. Tietoturvauhkien käsittely tutkimusaineistossa arkkitehtuurin osien mukaan luokiteltuna. 20

Sisältö

1 JOHDANTO 1

2 OHJELMISTO-OHJATTU TIETOVERKKOARKKITEHTUURI 3
2.1 Rakenne 3
2.2 Hyödyt 4
2.3 Tietoturva 5

3 OHJELMISTO-OHJATUN TIETOVERKKOARKKITEHTUURIN TIETOTURVAUHAT 7
3.1 Verkkoelementtitaso 9
3.2 Hallintataso 9
3.3 Verkkosovellustaso 10
3.4 Hallinta- ja verkkoelementtitasojen rajapinta 10
3.5 Verkkosovellus- ja hallintatasojen rajapinta 11

4 OHJELMISTO-OHJATUN TIETOVERKON JA PERINTEISEN TIETOVERKON TIETOTURVAUHAT 13

5 JOHTOPÄÄTÖKSET 15

LÄHTEET 17

LIITTEET 19
A Tietoturvauhkien käsittely tutkimusaineistossa 19

1 Johdanto

Tietoverkoilta vaadittavat ominaisuudet ovat muuttuneet viime vuosina. Mobiililaitteiden yleistyminen, pilvipalvelut ja virtuaalipalvelimet ovat luoneet uudenlaisia tarpeita. Perinteisen tietoverkon hierarkinen, asiakkaan ja palvelimen välillä tapahtuva viestintä on enää vain osa tietoliikenteestä, sillä nykyisissä verkoissa liikenne suuntautuu entistä enemmän horisontaalisesti palvelimelta palvelimelle: yhden sovelluksen tarvitsema tieto saatetaan hakea usealta eri palvelimelta.

Mobiililaitteiden määrä on lisääntynyt valtavasti, ja yritysten verkkoja käytetään monenlaisilla laitteilla eri paikoissa, ei pelkästään yrityksen sisällä. Siksi myös alueverkkojen liikenne lisääntyy. Lisäksi yritykset haluavat käyttää pilvipalveluiden resursseja joustavasti ja mukautuvasti, jolloin niiden saatavuus ja käytettävyys on tärkeää.

Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri (Software-Defined Networking, SDN) tarkoittaa tietoverkon hallitsemista ohjelmistolla. Verkkolaitteet vain välittävät liikennettä, ja varsinainen verkon älykkyys on keskitetty hallintatasolle. Tämä mahdollistaa laajankin tietoverkon hallinnan keskitetysti yhdestä paikasta. Lisäksi verkon infrastruktuuri voidaan piilottaa abstraktioihin, jotka tarjoavat käyttäjille räätälöidyn näkymän verkosta. Ohjelmisto-ohjatun tietoverkon toimintaa voidaan myös muuttaa reaaliaikaisesti SDN-sovelluksilla, joilla voidaan automatisoida verkon resurssien käyttöä. Keskitetyn älykkyyden ansiosta uusien palveluiden käyttöönotto on nopeampaa kuin perinteisessä tietoverkossa. (*Software-Defined Networking: The New Norm for Networks* 2012)

Perinteisen tietoverkon staattisuus ja jäykkyys on ongelma isoille datakeskuksille ja verkko-operaattoreille, sillä niiden tarpeet ovat alati muuttuvia ja vaihtelevia. Google aloitti oman alueverkkonsa muuttamisen ohjelmisto-ohjatuksi vuonna 2010. Googlen teknisen infrastruktuurin vanhemman varajohtajan Urs Hölzlen mukaan SDN-arkkitehtuurin avulla voidaan hallita yhtä yhtenäistä järjestelmää yksittäisten verkkolaitteiden sijaan. Lisäksi verkkoa voidaan simuloida helposti vikojen löytämiseksi ja korjaamiseksi jo ennen käyttöönottoa. Googlen ohjelmisto-ohjatun verkon käyttöaste on lähellä 100:a prosenttia, kun se tavallisesti on 30–40 prosenttia, joten uusi teknologia vähentää myös ylläpitokustannuksia. (Fewell 2012)

Myös sosiaalisen median suuryhtiö Facebook on ottanut ohjelmisto-ohjatun tietoverkkoarkkitehtuurin käyttöönsä. Najam Ahmad, Facebookin teknisten operaatioiden johtaja, sanoo verkon horisontaalisen skaalautuvuuden ja ketteryyden olevan arkkitehtuurin suurimpia hyötyjä. Lisäksi verkkoa voidaan hallita halutunlaisella sovelluksella sen sijaan, että käytettäisiin verkkolaitteen tarjoamaa rajapintaa. Ahmadin mielestä ohjelmisto-ohjattuun arkkitehtuuriin siirtyminen voi myös vähentää erityisten tietoverkko-osaajien tarvetta yrityksissä. (Kerner 2014)

Ohjelmisto-ohjatun tietoverkon tietoturvaan suhtaudutaan kahdella eri tavalla. Toisaalta, kuten tutkijat Schehlmann, Abt ja Baier (2014) toteavat, verkon keskitetty hallinta ja tietoturvaa parantavat sovellukset ovat arkkitehtuurille eduksi verrattuna perinteisiin tietoverkkoihin. Kuitenkin Scott-Hayward, O'Callaghan ja Sezer (2013) huomauttavat, että samat piirteet voivat olla myös tietoturvauhkia: keskitetty hallinta altistaa verkon palvelunestohyökkäyksille ja sovellusten ja ohjaimen välisen luottamuksen varmentaminen voi olla vaikeaa.

Tässä tutkielmassa haluttiin selvittää, millaisia tietoturvauhkia ohjelmisto-ohjatussa tietoverkkoarkkitehtuurissa on. Tutkimus toteutettiin systemaattisena kirjallisuuskatsauksena, jonka aineistoksi valituissa artikkeleissa kuvaillaan ohjelmisto-ohjatussa tietoverkkoarkkitehtuurissa esiintyviä tietoturvauhkia. Erityisesti haluttiin kartoittaa, kuinka kattavasti aiheen osa-alueita on tutkittu. Lisäksi selvitettiin ohjelmisto-ohjatun ja perinteisen tietoverkon tietoturvauhkien eroja. Tutkimuskysymykset ovat seuraavat:

1. Mitä tietoturvauhkia ohjelmisto-ohjatussa tietoverkkoarkkitehtuurissa on?
2. Missä arkkitehtuurin osissa tietoturva-aukot sijaitsevat?
3. Miten ohjelmisto-ohjatun tietoverkon ja perinteisen tietoverkon tietoturvauhat eroavat toisistaan?

Tutkielma etenee seuraavasti: Luvussa 2 tarkastellaan ohjelmisto-ohjatun tietoverkkoarkkitehtuurin rakennetta ja ominaisuuksia. Luvussa 3 kuvaillaan arkkitehtuurin tietoturvauhkia luokiteltuna sen mukaan, missä arkkitehtuurin osassa ne sijaitsevat. Ohjelmisto-ohjatun ja perinteisen tietoverkon tietoturvauhkia on vertailtu luvussa 4. Luvussa 5 esitetään johtopäätökset.

2 Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri

Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri (Software-Defined Networking, SDN) on uudehko tapa toteuttaa tietoverkkoja. Se on suunniteltu laajoille verkoille, joiden pitää olla helposti hallittavissa, reaaliajassa käyttäjien tarpeisiin mukautuvia ja tehokkaita. Tällaisia verkkoja ovat esimerkiksi suurten verkko-operaattoreiden verkot ja pilvipalvelut, joilla on paljon käyttäjiä. Arkkitehtuuria voidaan hyödyntää myös yritysten monimutkaisissa sisäisissä verkoissa.

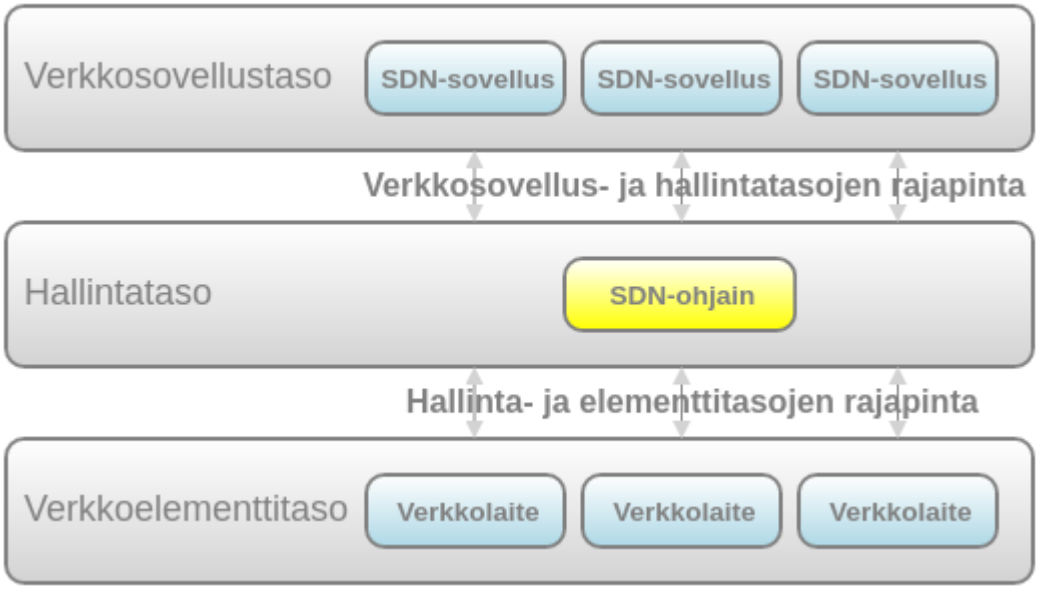
Ohjelmisto-ohjatussa tietoverkkoarkkitehtuurissa on kolme tasoa: verkkoelementtitaso, hallintataso ja verkkosovellustaso (ks. kuvio 1). Merkittävimpänä erona perinteisiin tietoverkkoihin voidaan pitää tietoliikenteen välittämisen ja verkon hallinnan erottamista toisistaan: hallintatason ohjain hallitsee koko verkkoa ja antaa reititysohjeita verkkolaitteille, jotka vain välittävät liikennettä. Lisäksi arkkitehtuuri hyödyntää SDN-sovelluksia, joiden avulla verkon toimintaa voidaan ohjata ja muuttaa reaaliaikaisesti.

2.1 Rakenne

Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri jaetaan kolmeen tasoon: verkkoelementtitaso, hallintataso ja verkkosovellustaso.

Arkkitehtuurin verkkoelementtitasolla (engl. infrastructure layer) sijaitsevat verkkolaitteet. Perinteisen tietoverkon verkkolaitteessa on kaksi tasoa: hallintakerros (engl. control plane) ja tiedonvälityskerros (engl. forwarding plane, data plane). Hallintakerros huolehtii muun muassa liikenteen ohjaamisesta ja reitityksestä, kun taas tiedonvälityskerroksella laitteeseen saapuneet paketit lähetetään eteenpäin hallintakerroksen ohjeiden mukaan. Ohjelmisto-ohjatussa tietoverkossa verkkolaitteen tarvitsee huolehtia vain tiedonvälityskerroksen velvollisuuksista, sillä kaikki reititykseen tarvittava tieto saadaan ylempää hallintatasolta.

Hallintatasolla (engl. control layer) toimii erityinen ohjelmisto, ohjain, jolla hallitaan koko tietoverkkoa. Jokainen verkkolaite yhdistetään ohjaimeen, joka välittää niille reititysohjeet. Ohjeet tallennetaan laitteen reititystauluun. Jos laite ei osaa reitittää saapunutta pakettia, se



Kuvio 1. Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin rakenne.

kysyy neuvoa ohjaimelta. Käytännön verkoissa ohjaimia on yleensä enemmän kuin yksi vikasietoisuuden parantamiseksi. Ohjaimen ja verkkolaitteen viestintää varten laitteen täytyy tukea jotakin SDN-arkkitehtuurin viestintäprotokollaa. Yksi tällainen protokolla on avoimen standardin OpenFlow (*OpenFlow* 2016).

Ohjain on myös yhteydessä SDN-sovelluksiin, jotka toimivat verkkosovellustasolla (engl. application layer). Sovellukset voivat esimerkiksi valvoa tietoliikennettä, hoitaa reititystä, hallinnoida resursseja ja parantaa tietoturvaa. Ohjain voi tarjota sovellukselle juuri sitä varten räätälöidyn abstraktion verkosta. Ohjaimen ja sovellusten välillä oleva rajapinta on avoin, joten sovelluksia voi kehittää kuka tahansa: sovelluskehittäjät, verkon ylläpitäjät tai käyttäjät. (*Software-Defined Networking: The New Norm for Networks* 2012)

2.2 Hyödyt

Ohjelmisto-ohjattu tietoverkko on skaalautuva, mukautuva ja helposti hallinnoitava. Nämä ominaisuudet tekevät siitä sopivan pilvilaskennan, verkko-operaattoreiden ja isojen yritysverkkojen tarpeisiin. Monissa tietoverkoissa verkon käyttäjien tarpeet muuttuvat nopeasti, jolloin ohjelmisto-ohjatun tietoverkon helposta hallinnasta on hyötyä: verkkoa voidaan hallita yksityiskohtaisesti istunto-, käyttäjä-, laite- ja sovellustasoilla ja resursseja voidaan ja-

kaa käyttöön tehokkaasti. Uusia palveluita ja ominaisuuksia voidaan ottaa käyttöön nopeasti. (*Software-Defined Networking: The New Norm for Networks* 2012) Ohjelmisto-ohjattu tietoverkko sopii hyvin myös virtualisoinnin tarpeisiin, sillä vaikka virtuaalisia palvelimia ja tietovarastoja voidaan luoda nopeasti, niiden käyttöönotto perinteisessä tietoverkossa voi olla hidasta. (*What's Software Defined Networking (SDN)? Definition* 2016)

Ohjelmistopohjaisuuden ansiosta ohjelmisto-ohjattu tietoverkko ei ole sidottu verkkolaitteiden valmistajien tarjoamiin laiteominaisuuksiin, vaan verkkoa rakennetaan ohjelmistojen avulla. Riittää, että verkkolaite toteuttaa jotakin arkkitehtuurin viestintäprotokollaa, jotta ohjaimen ja laitteen välinen viestintä onnistuu. Lisäksi ohjaimen ja SDN-sovellusten välisen rajapinnan avoimuuden ansiosta ohjelmisto-ohjattua verkkoa voidaan yksilöllistää räätälöidyillä sovelluksilla, joita voivat kehittää niin yritykset, palveluntarjoajat, sovelluskehittäjät kuin käyttäjätkin. (*Software-Defined Networking: The New Norm for Networks* 2012)

2.3 Tietoturva

Ohjelmisto-ohjattu tietoverkkoarkkitehtuuri voi parantaa myös verkon tietoturvaa. Koska verkkolaitteita hallitaan keskitetysti hallintatasolla, laitteiden konfiguraatiossa tehdään vähemmän virheitä. Lisäksi koko verkon kattava yhdenmukainen säännöstö helpottaa resurssien jakamista ja verkon käyttäytymisen hallintaa. (*Software-Defined Networking: The New Norm for Networks* 2012) Keskitetty hallinta pitää kuitenkin ottaa huomioon verkon tietoturvassa: ohjaimen suojaaminen hyökkäyksiltä on erityisen tärkeää. Myös ohjainten, laitteiden ja SDN-sovellusten luotettavuus pitää varmentaa. (*SDN Security Challenges in SDN Environments* 2016)

Scott-Hayward, O'Callaghan ja Sezer (2013) tunnistavat ohjelmisto-ohjatun tietoverkon tietoturvassa kaksi eri suhtautumistapaa. Toisaalta koko verkon kattava näkymä ja verkon ohjelmoitavuus mahdollistavat tiedon keräämisen esimerkiksi tunkeilijan havaitsemis- ja murronestämisjärjestelmistä ja verkon uudelleenohjelmoinnin tietojen analysoinnin perusteella. Tämä voi tehdä ohjelmisto-ohjatusta tietoverkosta turvallisemman perinteiseen tietoverkkoon verrattuna. Toisaalta samat ominaisuudet altistavat verkon uudenlaisille vaaroille, joiden torjumiseksi pitää löytää uusia keinoja.

Seuraavassa luvussa kuvaillaan tarkemmin ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhkia.

3 Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhat

Tässä luvussa kuvaillaan ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhkia. Uhat on luokiteltu sen mukaan, missä arkkitehtuurin osassa ne esiintyvät.

Tässä tutkielmassa kartoitettiin sellaista tutkimusta, jossa löydetyt tietoturvauhat esiintyvät kaikissa arkkitehtuurin tietoverkoissa eivätkä ole siis riippuvaisia esimerkiksi verkon toteutuksessa käytetyistä standardeista. Erityisesti haluttiin selvittää, mitä aiheen osa-alueita on jo tutkittu ja mitkä kaipaavat vielä lisätutkimusta. Tätä varten tutkimusmetodiksi valittiin systemaattinen kirjallisuuskartoitus, jonka avulla voidaan paljastaa jo tehdyn tutkimuksen mahdollisia puutteita (Salminen 2011). Lisäksi selvitettiin, miten ohjelmisto-ohjatun tietoverkon ja perinteisen tietoverkon tietoturvauhat eroavat toisistaan. Aineistoa haettiin ACM Digital Library-, IEEE Xplore Digital Library- ja Scopus-tietokannoista hakusanoilla "software-defined networking"ja "security". Aineistoon valittiin sellaiset artikkelit, joissa kuvaillaan ohjelmisto-ohjatussa tietoverkkoarkkitehtuurissa esiintyviä tietoturvauhkia. Artikkelit on esitetty taulukossa 1.

Vaikuttaa siltä, että ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvaa ei ole vielä tutkittu tarpeeksi. Esimerkiksi Kreutz, Ramos ja Verissimo (2013) ja Sezer ym. (2013, ss. 40–41) molemmat esittävät, että arkkitehtuurin laaja käyttöönotto edellyttää lisää tietoturvatutkimusta. Heidän mukaansa arkkitehtuurin monet tasot ja rajapinnat aiheuttavat enemmän mahdollisia tietoturva-aukkoja kuin tavallisissa tietoverkoissa. Myös Bétge-Brezetz, Kamga ja Tazi (2015) mainitsevat kerroksellisuudesta aiheutuvan mahdollisten uhkien lisääntymisen.

Arkkitehtuurin hyödyllisimmät ominaisuudet ovat ohjelmoitavuus ja hallinnan keskittäminen, mutta ne aiheuttavat myös vakavia tietoturvauhkia. Jesus ym. (2014, ss. 924–926) ovat arvioineet, että juuri arkkitehtuurin ohjelmistopohjaisuus voi olla merkittävä tietoturvariski, sillä ohjelmistoissa on omat ongelmansa: ohjelmavirheet, suorituksenaikaiset virheet, matala suoritusteho sekä toiminnallisuuden ja arkkitehtuurin puutteet. Turvallisuuteen vaikuttaa myös ohjelmiston konfiguraatio, jossa voi olla virheitä. Samat tutkijat korostavat myös sovel-

Taulukko 1. Kirjallisuuskartoitukseen valitut artikkelit.

Tekijä	Vuosi	Julkaisun nimi	Tietokanta
Akhunzada, A. ym.	2015	"Securing software defined networks: taxonomy, requirements, and open issues"	IEEE
Bétge-Brezetz, S. ym.	2015	"Trust support for SDN controllers and virtualized network applications"	IEEE
Jesus, W. Paim de ym.	2014	"Analysis of SDN Contributions for Cloud Computing Security"	ACM
Kreutz, D. ym.	2013	"Towards Secure and Dependable Software-defined Networks"	ACM
Schehlmann, L. ym.	2014	"Blessing or curse? Revisiting security aspects of Software-Defined Networking"	IEEE
Scott-Hayward, S. ym.	2013	"SDN Security: A Survey"	IEEE
Sezer, S. ym.	2013	"Are we ready for SDN? Implementation challenges for software-defined networks"	IEEE

luksen ja ohjaimen sekä ohjaimen ja verkkolaitteen välisen viestinnän turvaamisen tärkeyttä.

Monet tutkijat ottavat kantaa myös tulevaan tutkimukseen. Tutkijoitten Schehlmann, Abt ja Baier (2014) mielestä seuraavaksi pitäisi selvittää, miten jo olemassa olevia tietoturvaratkaisuja voidaan soveltaa ohjelmisto-ohjattuihin tietoverkkoihin. Kreutz, Ramos ja Verissimo (2013) taas korostavat arkkitehtuurin uudenlaisia uhkia, jotka vaativat omat ratkaisunsa. He myös pitävät arkkitehtuurin oman tietoturvan parantamista tärkeämpänä kuin ulkopuolisten ratkaisujen kehittämistä.

Tutkimuksessa löydetyt ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhat on esitetty taulukossa 2. Seuraavissa alaluvuissa tietoturvauhkia kuvaillaan tarkemmin. Uhat on esitetty arkkitehtuurin kolmen tason ja kahden rajapinnan mukaisesti luokiteltuna.

3.1 Verkkoelementtitaso

Arkkitehtuurin verkkoelementtitasolla on havaittu palvelunestohyökkäyksen uhka. Sezer ym. (2013, ss. 40–41) esittävät palvelunestohyökkäyksen muodon, jossa käytetään hyödyksi reititysohjeiden pyytämistä ohjaimelta. Kun verkkolaitteeseen saapuu paketti, jonka reititysohjeita ei löydy reititystaulusta, laite pyytää ohjeita ohjaimelta. Laite lähettää ohjaimelle joko koko paketin tai vain paketin otsakkeet, jolloin paketin data tallennetaan verkkolaitteen muistiin. Jälkimmäisessä tapauksessa laitteen muisti voi täyttyä pakettien datasta, jos tällaisia paketteja saapuu tiheään. Muistin loppuessa se ei voi enää välittää liikennettä.

Tutkijoitten Kreutz, Ramos ja Verissimo (2013) mukaan palvelunestohyökkäys voidaan toteuttaa myös väärentämällä tai muokkaamalla tietoliikennettä. Liikenteen vääristelyssä käytetään hyödyksi kaapattuja verkkolaitteita. Kaapattu verkkolaite voi myös tarkoituksella hukata tai monistaa paketteja tai hidastaa niiden kulkua, jolloin hyökkääjä voi varastaa laitteen kautta kulkevaa tietoa.

Verkkolaitteiden ohjelmistoihin ovat kiinnittäneet huomionsa tutkijat Akhunzada ym. (2015). Ohjelmisto saattaa olla virheellisesti toteutettu tai sen toimintaa voidaan muuttaa hyökkääjän eduksi. Heidän mukaansa myös fyysisen laitteiston häiriöt on otettava huomioon verkon turvallisuudessa.

3.2 Hallintataso

Monessa artikkelissa on kiinnitetty huomiota ohjaimeen kohdistuviin tietoturvauhkiin. Arkkitehtuurissa tehdyn ratkaisun erottaa hallinta- ja tiedonvälityskerros toisistaan katsotaan aiheuttavan myös haittaa tietoturvalle. Tutkijoitten Sezer ym. (2013, ss. 40–41) mukaan arkkitehtuurin ohjain on erittäin houkutteleva hyökkäyksen kohde sille keskitetyn verkon hallinnan takia. Kreutz, Ramos ja Verissimo (2013) pitävät ohjaimen haavoittuvuuksia ja siihen kohdistuvia hyökkäyksiä vakavana uhkana, koska kaapattu ohjain voi vaarantaa koko tietoverkon. Juuri näistä syistä tutkijat Bétge-Brezetz, Kamga ja Tazi (2015) ovat sitä mieltä, että ohjaimelle on annettu liikaa valtaa. Sezer ym. (2013, ss. 40–41) esittävät huolensa myös siitä, mitä tapahtuu, jos ohjaimen saatavuudessa on katkoja, sillä verkkolaitteet tarvitsevat ohjaimelta tulevia ohjeita reititystaulussa määrittelemättömien pakettien välittämiseen.

Ohjaimen valtakeskittymän lisäksi esitetään muitakin ohjaimeen liittyviä uhkia. Sekä Sezer ym. (2013, ss. 40–41) että Akhunzada ym. (2015) esittävät, että hyökkääjä saattaa luoda väärennetyn ohjaimen ja päästä sen kautta aiheuttamaan vahinkoa verkossa. Lisäksi Akhunzada ym. (2015) ja Jesus ym. (2014, ss. 924–926) ovat kiinnittäneet huomionsa ohjaimen ohjelmistopohjaisuuteen ja ohjelmistoille tyypillisiin ongelmiin: ohjelmistossa saattaa olla virheitä tai sen toimintaa voidaan muutttaa hyökkääjän tarpeisiin sopivaksi.

3.3 Verkkosovellustaso

Verkkosovellustasolla Scott-Hayward, O'Callaghan ja Sezer (2013) tuovat esiin haitallisiin SDN-sovelluksiin liittyvän ongelman: koska sovellusten aitoutta ei varmisteta, hyökkäystarkoituksiin tehty sovellus saatetaan tietämättä ottaa käyttöön. Haitallisella sovelluksella voidaan esimerkiksi muuttaa verkon säännöstöä hyökkääjälle suotuisaksi tai antaa vääriä reititysohjeita ohjaimelle.

Tutkijat Sezer ym. (2013, ss. 40–41) kiinnittivät huomionsa usean SDN-sovelluksen yhteistoimintaan. Heidän mukaansa reititysohjeet eivät välttämättä pysy ristiriidattomina, jos niitä antaa useampi sovellus, koska mahdollisia ristiriitoja ei tarkisteta missään vaiheessa ohjaimen ja sovellusten välillä.

3.4 Hallinta- ja verkkoelementtitasojen rajapinta

Hallinta- ja verkkoelementtitasojen rajapinnassa tutkijat ovat perehtyneet ohjaimen ja verkkolaitteen viestinnässä käytettyjen protokollien tietoturvaan. Tutkijoitten Sezer ym. (2013, ss. 40–41) mukaan verkkolaitteen aitous on todennettava, kun se yhdistetään ohjaimeen. Tällä tavalla varmistetaan yhteyden turvallisuus ja liikenteen suojaaminen. Tutkijat vaativat ohjaimen ja verkkolaitteen välisen rajapinnan turvallisuuden tarkkaa määrittelyä, sillä tällä hetkellä esimerkiksi OpenFlow'n spesifikaatioissa TLS (Transport Layer Security) -salausprotokollan käyttö ei ole pakollista. Heidän mukaansa TLS:n tuoma turva saattaa riittää yhden ohjaimen tapauksessa, mutta jos useampi ohjain viestii saman verkkolaitteen kanssa tai monta hallintaprosessia yhden keskitetyn ohjaimen kanssa, oikeuksien jakaminen ja pääsynhallinta monimutkaistuu. (Sezer ym. 2013, ss. 40–41) Kreutz, Ramos ja Verissimo

(2013) huomauttavat vielä, että on yleisesti tunnettua, että edes TLS ei takaa turvallista viestintää, koska siitä ja sen käyttämästä julkisten avainten hallintajärjestelmästä (Public Key Infrastructure, PKI) on löydetty heikkouksia. Heidän mielestään TLS ei riitä varmentamaan ohjaimen ja verkkolaitteen yhteyttä.

Kreutz, Ramos ja Verissimo (2013) ovat kiinnittäneet huomionsa ohjaimen ja verkkolaitteen välisten protokollien määrään. Protokollia on ainakin vielä melko vähän, ja samaa protokollaa käytetään yleensä koko verkossa. Tutkijoitten mukaan tästä syystä yhden protokollan virheet tai puutteet voivat vaarantaa kokonaisen verkon. (Kreutz, Ramos ja Verissimo 2013)

3.5 Verkkosovellus- ja hallintatasojen rajapinta

Sovellus- ja hallintatasojen rajapinnan tietoturvauhat liittyvät rajapinnan avoimuuteen ja SDN-sovellusten aitouden todentamiseen. Kreutz, Ramos ja Verissimo (2013) huomauttavat, että avoin rajapinta antaa kenelle tahansa mahdollisuuden kehittää ja levittää haitallisia sovelluksia. Sezer ym. (2013, ss. 40–41) taas pitävät avoimia rajapintoja ja protokollia uhkana siitä syystä, että ne tekevät verkon rakenteesta ja toiminnasta julkista tietoa. Tietojen avulla tietoverkko voidaan helposti ja nopeasti muuttaa hyökkääjälle hyödylliseksi välineeksi, jos hyökkääjällä on pääsy ohjaimeen. Myös yksittäiset verkkolaitteet, päätelaitteet ja käyttäjät voivat olla tällaisen hyökkäyksen kohteita.

SDN-sovellusten aitouden todentaminen ei tutkijoitten Schehlmann, Abt ja Baier (2014) mielestä pitäisi olla vaikeaa, koska siihen on jo kehitetty erilaisia keinoja. Niitä ei ole kuitenkaan sisällytetty arkkitehtuuriin itseensä, kuten myös Kreutz, Ramos ja Verissimo (2013) huomauttavat. Sezer ym. (2013, ss. 40–41) tuovat saman asian esille viitatessaan jo vanhentuneeseen IETF:n julkaisemaan Internet-vedokseen (Hartman ja Zhang 2013), jonka mukaan arkkitehtuurissa tarvitaan keinoja SDN-sovellusten aitouden varmentamiseksi.

Taulukko 2. Ohjelmisto-ohjatun tietoverkkoarkkitehtuurin tietoturvauhkia.

Taso/rajapinta	Uhka
Verkkosovellustaso	Haitalliset SDN-sovellukset
	Usean SDN-sovelluksen antamien reititysohjeiden ristiriidattomuus
Hallintataso	Ohjaimelle keskitetty verkon hallinta
	Katkot ohjaimen saatavuudessa
	Väärennetty ohjain
	Ohjaimen ohjelmiston viat ja puutteet
Verkkoelementtitataso	Verkkolaitteen muistin loppumista hyödyöntävä palvelunestohyökkäys
	Kaapattua verkkolaitetta hyödyntävä palvelunestohyökkäys
	Verkkolaitteen ohjelmiston viat ja puutteet
	Fyysisen laitteiston häiriöt
Verkkosovellus- ja hallintatason rajapinta	Rajapinnan avoimuus
	Protokollien avoimuus
	SDN-sovelluksen aitouden todentamattomuus
Hallinta- ja verkkoelementtitason rajapinta	Verkkolaitteen aitouden todentamattomuus
	Protokollien puutteellinen tietoturvakeinojen määrittely
	Protokollien vähäinen määrä

4 Ohjelmisto-ohjatun tietoverkon ja perinteisen tietoverkon tietoturvauhat

Ohjelmisto-ohjatun tietoverkon tietoturvallisuutta on myös verrattu perinteiseen tietoverkkoon. Perinteisellä tietoverkolla tarkoitetaan verkkoa, joka koostuu verkkolaitteista, joissa jokaisessa on sekä hallintakerros että tiedonvälityskerros. Ohjelmisto-ohjatussa tietoverkossa nämä kerrokset on erotettu toisistaan toteuttamalla erillinen ohjain ja jättämällä verkkolaitteen tehtäväksi vain liikenteen välittämisen.

Kreutz, Ramos ja Verissimo (2013) ovat kiinnittäneet huomionsa juuri hallinta- ja tiedonvälityskerrosten erottamiseen: hyökkääjän pääsy käsiksi hallintakerrokseen on ohjelmisto-ohjatussa verkossa paljon suurempi uhka kuin perinteisessä verkossa, koska hallintakerroksen ohjaimen kautta voidaan hallita koko tietoverkkoa yksittäisen verkkolaitteen sijaan. Samojen tutkijoiden mukaan myös vaarantunut verkkolaite on suurempi uhka ohjelmisto-ohjatussa verkossa kuin perinteisessä. Myös Schehlmann, Abt ja Baier (2014) pitävät ohjainta keskeisenä ohjelmisto-ohjatun verkon turvallisuudessa. Ohjaimen tulee olla saatavissa aina tarvittaessa, sillä verkkolaitteet pyytävät ohjaimelta reititysohjeita paketeille, jotka eivät sovi laitteiden omien reititystaulujen sääntöihin. Verkkolaitteiden käyttökatkot eivät taas ole niin vakavia, sillä ohjain voi reitittää liikenteen uudelleen käyttäen toimivia laitteita, mikä on työlästä perinteisessä tietoverkossa. Arkkitehtuurin kerroksellisuus taas vaatii kerrosten välillä kulkevien viestien suojaamista salakuuntelulta ja muokkaamiselta. Tutkijat huomauttavatkin, että perinteiset tietoverkot ovat joiltain osin turvallisempia juuri siksi, että niistä puuttuu ohjelmisto-ohjatun verkkoarkkitehtuurin ohjaimet ja SDN-sovellukset, joita voidaan käyttää hyväksi hyökkäyksissä. (Schehlmann, Abt ja Baier 2014)

Tutkijoitten Jesus ym. (2014, ss. 924–926) mukaan ohjelmisto-ohjatun tietoverkon ohjelmistopohjaisuus voi olla merkittävä tietoturvariski. Ohjelmistoissa voi olla ohjelmointivirheitä tai puutteita arkkitehtuurissa tai toiminnallisuudessa. Lisäksi ohjelmia suoritettaessa voi tapahtua virheitä tai suorittaminen voi olla tehotonta. (Jesus ym. 2014, ss. 924–926) Kreutz, Ramos ja Verissimo (2013) huomauttavat, että perinteisen verkon verkkolaitteen ohjelmistossa viat ja puutteet eivät aiheuta niin vakavia seurauksia, koska eri laitteita on huomat-

tavasti enemmän kuin esimerkiksi ohjelmisto-ohjatun arkkitehtuurin ohjainohjelmistoja ja protokollia. Viallinen ohjelmisto vaarantaa perinteisessä verkossa vain kyseistä ohjelmistoa käyttävät laitteet, kun taas ohjelmisto-ohjatussa verkossa laitteiden ja ohjelmistojen kirjo on paljon suppeampi ja viallisuus voi vaikuttaa laajaltikin.

Toisaalta monet tietoturvauhat esiintyvät sekä perinteisissä että ohjelmisto-ohjatuissa tietoverkoissa. Tutkijat Schehlmann, Abt ja Baier (2014) ovat tunnistaneet useita tietoturvaongelmia, jotka ovat samankaltaisia molemmissa verkoissa. Ongelmat viestinnän salaamisessa, pääsynhallinnassa ja verkkolaitteiden todentamisessa esiintyvät kaikissa tietoverkoissa, mutta niihin voidaan soveltaa olemassa olevia keinoja riippumatta verkon arkkitehtuurista. Samojen tutkijoiden mukaan myös reititysohjeiden eheyden turvaaminen ja niiden ristiriidattomuus on yhtä tärkeää molemmissa verkoissa. Schehlmann, Abt ja Baier (2014) uskovatkin, että ohjelmisto-ohjatun tietoverkon tietoturvauhat eivät ole täysin uudenlaisia, vaan niiden ratkaisemiseksi voidaan käyttää jo olemassa olevia tekniikoita.

5 Johtopäätökset

Tämän tutkielman tarkoituksena oli löytää tietoturvauhkia ohjelmisto-ohjatusta tietoverkkoarkkitehtuurista kirjallisuuskartoituksen keinoin. Tutkimuksessa kävi ilmi, että tietoturvauhkia on tunnistettu kaikista arkkitehtuurin tasoista ja rajapinnoista. Verkkosovellustasolla uhkia esiintyi kaksi, hallinta- ja sovellustasojen sekä hallinta- ja verkkoelementtitasojen rajapinnoissa kolme ja hallinta- ja verkkoelementtitasoilla neljä. Löydetyt uhat sijaitsevat siis melko tasaisesti koko arkkitehtuurissa. Tietoturvauhkien määrä saattaa kertoa joko arkkitehtuurin turvallisuudesta tai tehdyn tutkimuksen kattavuudesta.

Monessa tutkimuksessa oli esillä erityisesti hallintatason tietoturva ja nimenomaan ohjaimesta löydetyt ongelmat. Arkkitehtuurissa tehtyä ratkaisua erottaa hallinta- ja tiedonvälityskerros toisistaan pidettiin sekä tietoturvaetuna että -haittana: toisaalta ohjaimeen keskitetty hallinta helpottaa tietoverkon hallintaa ja valvontaa, mutta toisaalta ohjaimesta tulee erittäin houkutteleva hyökkäyksen kohde, jonka kautta voidaan päästä käsiksi koko tietoverkkoon. Lisäksi ohjainohjelmisto on alttiina kaikille ohjelmistoille tyypillisille vioille ja puutteille, jotka voivat aiheuttaa tietoturvaongelmia. Arkkitehtuurin hallintatason tietoturvaa voitaneen pitää erityisen tärkeänä, koska ohjaimen vaarantumisella voi olla vakavat seuraukset.

Arkkitehtuurin rajapinnoista löydetyt tietoturvauhat liittyvät arkkitehtuurin kerroksien välisen viestinnän suojaamiseen ja verkon elementtien aitouden todentamiseen. Sekä SDN-sovelluksen ja ohjaimen että ohjaimen ja verkkolaitteen väliset yhteydet täytyy suojata, jotta vältytään esimerkiksi liikenteen salakuuntelulta. Arkkitehtuurissa ei oteta kantaa näiden yhteyksien suojaamiseen, joten käytettyjen viestintäprotokollien tulee olla turvallisia. SDN-sovellusten ja verkkolaitteiden aitouden varmentamisella taas voidaan estää haitallisten sovellusten ja laitteiden pääsy verkkoon, minkä torjumiseksi on käytettävä ulkopuolisia ratkaisuja. Rajapintojen tietoturva riippunee pitkälti käytetyistä viestintäprotokollista.

Tutkielmassa verrattiin myös ohjelmisto-ohjatun tietoverkon ja perinteisen tietoverkon tietoturvauhkia keskenään. Kreutz, Ramos ja Verissimo (2013), Bétge-Brezetz, Kamga ja Tazi (2015) ja Sezer ym. (2013) ovat sitä mieltä, että arkkitehtuurin kerroksellisuus saattaa aiheuttaa lisää tietoturvauhkia perinteiseen tietoverkkoon verrattuna, minkä vuoksi ohjelmisto-

ohjatun tietoverkon tietoturvaa on syytä tarkastella erillään perinteisestä tietoverkosta. Kuitenkin Schehlmann, Abt ja Baier (2014) tulivat tutkimuksessaan siihen tulokseen, että ohjelmisto-ohjattu tietoverkko on perinteistä verkkoa turvallisempi. Vaikka ohjelmisto-ohjatussa tietoverkossa on tietoturvauhille altistavia ominaisuuksia, kuten kerroksellisuus ja verkon hallinnan keskittäminen, siitä voidaan tehdä turvallinen esimerkiksi SDN-sovellusten ja rajapintojen protokollien avulla. Lienee kuitenkin tärkeää tiedostaa ohjelmisto-ohjatun ja perinteisen tietoverkon olennaisimmat erot ja niiden vaikutukset tietoturvaratkaisuihin.

Liitteessä A taulukossa 3 on esitetty, mitä arkkitehtuurin osaa missäkin kirjallisuuskartoituksessa mukana olevassa artikkelissa on käsitelty. Määrällisesti tutkimuksissa on käsitelty eniten hallintatason ja verkkosovellus- ja hallintatasojen rajapinnan tietoturvaongelmia ja hieman vähemmän verkkosovellus- ja verkkoelementtitasoa ja hallinta- ja verkkoelementtitasojen rajapintaa. Tämän perusteella vaikuttaa siltä, että tarvetta jatkotutkimuksille on vielä erityisesti verkkosovellus- ja verkkoelementtitasojen sekä hallinta- ja verkkoelementtitason rajapinnan tietoturvassa. Tutkimusta on kuitenkin tehty melko tasaisesti koko arkkitehtuurista.

Lähteet

Akhunzada, A., E. Ahmed, A. Gani, M. Khan, M. Imran ja S. Guizani. 2015. “Securing software defined networks: taxonomy, requirements, and open issues”. *IEEE Communications Magazine* 53 (4): 36–44.

Bétge-Brezetz, S., G.-B. Kamga ja M. Tazi. 2015. “Trust support for SDN controllers and virtualized network applications”. Teoksessa *2015 1st IEEE Conference on Network Softwarization (NetSoft),* 1–5. IEEE.

Fewell, Art. 2012. “Google Showcases OpenFlow network”. URL: `http://www.networkworld.com/article/2222173/cisco-subnet/google-showcases-openflow-network.html`. Viitattu 10.3.2016, *Network World.*

Hartman, Sam D., ja Dacheng Zhang. 2013. *Security Requirements in the Software Defined Networking Model.* Tekninen raportti. Internet-vedos, vanhentunut. Internet Engineering Task Force.

Jesus, W. Paim de, D. Alves da Silva, R. T. de Sousa ja F. V. Lopes Da Frota. 2014. “Analysis of SDN Contributions for Cloud Computing Security”. Teoksessa *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC),* 922–927. IEEE.

Kerner, Sean Michael. 2014. “Why Fasebook Does SDN”. URL: `http://www.enterprisenetworkingplanet.com/datacenter/why-facebook-does-sdn.html`. Viitattu 11.3.2016, *Enterprise Networking Planet.*

Kreutz, Diego, Fernando M. V. Ramos ja Paulo Verissimo. 2013. “Towards Secure and Dependable Software-defined Networks”. Teoksessa *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking,* 55–60. HotSDN ’13. New York, NY, USA: ACM.

OpenFlow. 2016. URL: `https://www.opennetworking.org/sdn-resources/openflow`. Viitattu 12.2.2016.

Salminen, Ari. 2011. “Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin”. Luku Systemaattinen kirjallisuuskatsaus, 9–11. Vaasa: Vaasan yliopiston julkaisuja. Opetusjulkaisuja 62, Julkisjohtaminen 4.

Schehlmann, L., S. Abt ja H. Baier. 2014. “Blessing or curse? Revisiting security aspects of Software-Defined Networking”. Teoksessa *Proceedings of the 10th International Conference on Network and Service Management (CNSM),* 382–387. IEEE.

Scott-Hayward, S., G. O’Callaghan ja S. Sezer. 2013. “SDN Security: A Survey”. Teoksessa *2013 IEEE SDN for Future Networks and Services (SDN4FNS),* 1–7. IEEE.

SDN Security Challenges in SDN Environments. 2016. URL: `https://www.sdxcentral.com/resources/security/security-challenges-sdn-software-defined-networks/`. Viitattu 23.3.2016.

Sezer, S., S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller ja N. Rao. 2013. “Are we ready for SDN? Implementation challenges for software-defined networks”. *IEEE Communications Magazine* 51 (7): 36–43.

Software-Defined Networking: The New Norm for Networks. 2012. ONF White Paper. URL: `https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf`. Viitattu 12.2.2016.

What’s Software Defined Networking (SDN)? Definition. 2016. URL: `https://www.sdxcentral.com/resources/sdn/what-the-definition-of-software-defined-networking-sdn/`. Viitattu 23.3.2016.

Liitteet

A Tietoturvauhkien käsittely tutkimusaineistossa

Taulukko 3. Tietoturvauhkien käsittely tutkimusaineistossa arkkitehtuurin osien mukaan luokiteltuna.

Taso/rajapinta	Artikkeli
Verkkoelementtitataso	Akhunzada ym. (2015) Kreutz, Ramos ja Verissimo (2013) Schehlmann, Abt ja Baier (2014) Scott-Hayward, O'Callaghan ja Sezer (2013) Sezer ym. (2013)
Hallintataso	Akhunzada ym. (2015) Bétge-Brezetz, Kamga ja Tazi (2015) Jesus ym. (2014) Kreutz, Ramos ja Verissimo (2013) Schehlmann, Abt ja Baier (2014) Scott-Hayward, O'Callaghan ja Sezer (2013) Sezer ym. (2013)
Verkkosovellustaso	Akhunzada ym. (2015) Bétge-Brezetz, Kamga ja Tazi (2015) Schehlmann, Abt ja Baier (2014) Scott-Hayward, O'Callaghan ja Sezer (2013) Sezer ym. (2013)
Hallinta- ja verkkoelementtitasojen rajapinta	Akhunzada ym. (2015) Jesus ym. (2014) Kreutz, Ramos ja Verissimo (2013) Schehlmann, Abt ja Baier (2014) Sezer ym. (2013)
Verkkosovellus- ja hallintatasojen rajapinta	Akhunzada ym. (2015) Bétge-Brezetz, Kamga ja Tazi (2015) Jesus ym. (2014) Kreutz, Ramos ja Verissimo (2013) Schehlmann, Abt ja Baier (2014) Scott-Hayward, O'Callaghan ja Sezer (2013) Sezer ym. (2013)