

Luottamus ja esineiden internet



Luottamus ja esineiden internet

IoT (Internet of Things), eli suomeksi esineiden internet tuo uusia liiketoimintamahdollisuuksia perinteisille aloille, mutta myös mahdollisuuden luoda täysin uusia liiketoimintoja.

Esineiden internet verkottaa kodin ja erilaiset älylaitteet terveystietojen, älykkäisiin kodinkoneisiin, muokaten kuluttajien ja yritysten arkea tulevaisuudessa. Vuonna 2020 kuluttajien ennustetaan investoivan IoT-bisnekseen 236 miljardia dollaria ja yritysten peräti 832 miljardia dollaria¹⁾.

Kun uusia liiketoimia luodaan IoT:n avulla, on datan luotettavuuden ja oikeellisuuden varmistaminen ensisijaisen tärkeää. Tämä korostuu entisestään tulevaisuudessa EU:n tietosuojasäätöjen astuessa voimaan. Yhtä tärkeää on myös laitteiden tietoturvallisuuden ja tietoturva-ominaisuuksien hallinta läpi

niiden elinkaaren. Suomalaisista organisaatioista 65 prosenttia²⁾ ei ole ottanut käyttöön suunnitelmaa tietoturva-ominaisuuksien hallintaa varten.

Kuinka luottaa laitteeseen ja sen lähettämään dataan, josta kenties koko liiketoiminta synnytetään? Liiketoimintojen perustuessa entistä enemmän järjestelmiin ja koneellisiin prosesseihin tulee näiden olla luotettavia ja tarpeen vaatien myös auditoituja. Yritysten tulee muotoilla liiketoimintastrategiansa ja -filosofiansa osittain uudelleen vastaamaan teollisen esineiden internetin (IIoT) hyödyntämistä. Uudenlaiset tavat hyödyntää teknologiaa vaativat strategista näkemystä ja prosesseja alati kehittyvän teknologian hallintaan.

Luottamusta vai uhkakuvia

Luottamuksen määrittely on haasteellinen ongelma, ja se korostuu erityisesti verkottuneessa IoT-maailmassa.

Internet of Things -sovellutuksen rakennetta tarkastellessa huomataan sen olevan hyvin pitkälle IT-infrastruktuuriin, missä muutkin olemassa olevat järjestelmät. Laite-isäntä-malli on voimissaan, ja verkot yhdistävät yhä laajempia alueita toisiinsa liiketoiminnassa. Esineiden internetissä korostuvat erityispiirteinä laitteiden runsas määrä ja niiden rajallinen prosessointiteho sekä laitteiden aktiivisen ylläpidon ja päivittämisen puuttuminen. Kuten missä tahansa IT-ympäristössä tietomurron riski on laitteesta riippumatta olemassa, jos ympäristöä ei ole asianmukaisesti suojattu. Tietomurrot aiheuttavat potentiaalisesti vakavia toiminnallisia häiriöitä. Murron suorien vaikutusten lisäksi merkittävää haittaa aiheuttaa laitteiden tarkastuksista ja korvaamisesta uusilla.

Uhkana on laitteiden yksinkertaisempi ja rajoittuneempi rakenne, joka tekee niistä

Yksinkertaistettu IoT-sovellutuksen rakenne



1) BI Intelligence, THE INTERNET OF THINGS 2015: Examining How The IoT Will Affect The World, November 2015

2) PwC Global Economic Crime Survey 2016 (www.pwc.com/crimesurvey)

jopa suuremman kiinnostuksen kohteen väärinkäytöksiä ja haittaohjelmia ajatellen. Halvan hinnan ollessa laitteiden suunnittelun lähtökohtana laitteiden suojaukseen panostetaan usein jo suunnitteluvaiheessa liian vähän. Yhdistämällä suuria määriä vähätehoisia laitteita bottiverkoiksi laitteista saadaan ulos riittävä määrä tehoja, jolloin väärinkäytösten kuten kryptovaluuttojen louhinnan tai verkkohyökkäysten toteuttamisesta tulee houkuttelevaa. Hakkerit ovat kiinnostuneita mahdollisuuksista väärinkäyttää puutteellisesti suojattuja laitteita. Laitteet ovat monesti myös osana esimerkiksi tuotantoa ohjaavia prosesseja, jolloin prosessien toiminta voi usein häiriintyä prosessointi-

tehojen ja resurssien kohdistuessa eri käyttötarkoituksiin.

Suuri osa IoT-maailman haasteista on läsnä nykyisissä IT-infrastruktuureissa, mutta itse laitteiden olemassaolo ja niiden monisuurtaisen verkottumisen laskeutuminen ruohonjuuritasolle luo tarpeen hallita esineiden internetin infrastruktuuria omana kokonaisuutena. Poikkeuksena aiempiin järjestelmiin esiin nousevat IoT-laitteiden uudet, joskus omintakeisetkin, protokollat verkkoviestinnässä, jotka hetkittäin aiheuttavat haasteita niin verkkosuunnittelulle kuin suojaukselle. IoT-maailma elää myös huomattavasti joustavammin: IoT-ekosysteemit rakennetaan usein niin, että

laitteet toimivat dynaamisesti elävässä infrastruktuurissa avoimia rajapintoja hyödyntäen, jotta muutoksia voidaan toteuttaa tiheästi.

Luottamuksen tarpeen määrittely

Kuinka voimme luottaa IoT-laitteeseen tai -anturiin? Kuinka voimme varmistua siitä että laitteen anturit lähettävät autenttista dataa? Tarvitseeko laitteeseen ylipäättään voida luottaa, ja mikä on pahin mahdollinen tilanne, jos luottamus laitteeseen katoaa?

Jotta näihin kysymyksiin voidaan vastata, täytyy tunnistaa millaisesta IoT-laitteiden infrastruktuurista on kyse.

Muutamia kysymyksiä järjestelmän luottamusvaatimusten määrittelyyn

Laitteen funktio ja vikatilanteet

- Ohjaavatko vai monitoroivatko IoT-laitteet prosessia?
- Onko ulkopuolisilla pääsyä antureihin?
- Mitä anturin vikaantumisesta seuraa?
- Varmistutaanko anturin datan oikeellisuudesta?
- Onko antureissa vikadiagnostiikkaa?

Järjestelmän redundanssi

- Tarvitseeko yksittäiseen laitteeseen luottaa?
- Miten yksittäinen sensori vaikuttaa pahimmassa tapauksessa koko prosessin toimintaan?
- Kuinka monen sensorin vikaantuminen alkaa häiritä toimintaa?
- Kuinka käsittelemme virheitä?
- Kuinka toivumme virheistä?

Integraation taso

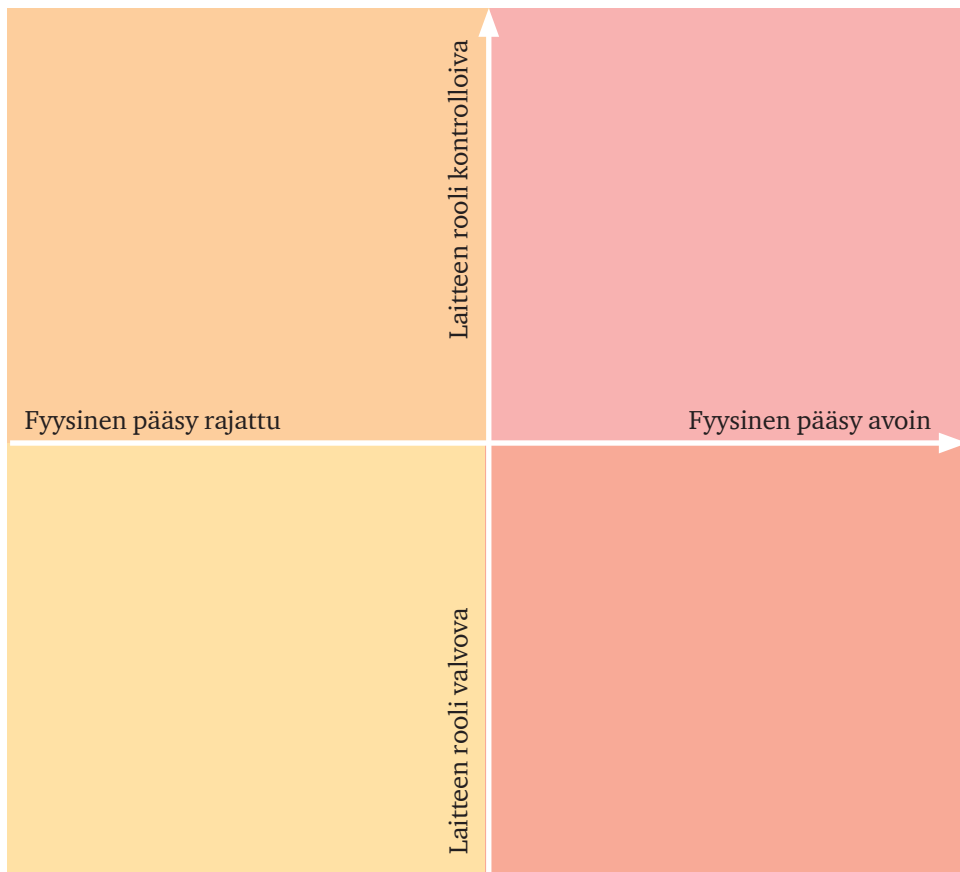
- Onko tiedossa hyökkäysvektoreita sensoreita tai järjestelmää vastaan?
- Mitä kautta järjestelmään voi kohdistua riskejä?
- Mikä on IoT-järjestelmän suhde muuhun IT-infrastruktuuriin?
- Kuinka IoT-järjestelmän osat on eriytetty toisistaan ja muusta IT-infrastruktuurista?
- Millainen pääsy laitteilla on muuhun IT-infrastruktuuriin?
- Millaisia hallinta- ja valvontakeinoja IoT-järjestelmässä on käytössä?

Laitteiden elinkaari ja hallintaprosessit

- Kuinka vikaantunut laite tunnistetaan ja huolletaan?
- Kuinka laitteet päivitetään?
- Miten järjestelmään tehdyt muutokset dokumentoidaan?
- Onko vaatimuksia järjestelmän toiminnalle ja elinkaaren hallinnalle määritelty?
- Onko järjestelmää tai toimintaprosesseja varmennettu tai auditoitu?

IoT-laitteiden luokitteluun voidaan käyttää esimerkiksi oheisia *laitteen fyysisen suojauksen kriittisyyden tunnistamisen* ja *laitteen toiminnan kriittisyyden tunnistamisen* nelikenttiä havainnollistamaan eri IoT-laitteiden ja niiden sensoreiden kriittisyyttä:

Laitteen fyysisen suojauksen kriittisyyden tunnistaminen



Mikäli järjestelmän laitteita tai antureita sijoittuu nelikenttien oikeaan yläkulmaan, on tärkeää kiinnittää huomiota niiden asemaan järjestelmässä sekä ottaa tämä huomioon riskienhallinnassa.

Keinoja luottamuksen luontiin

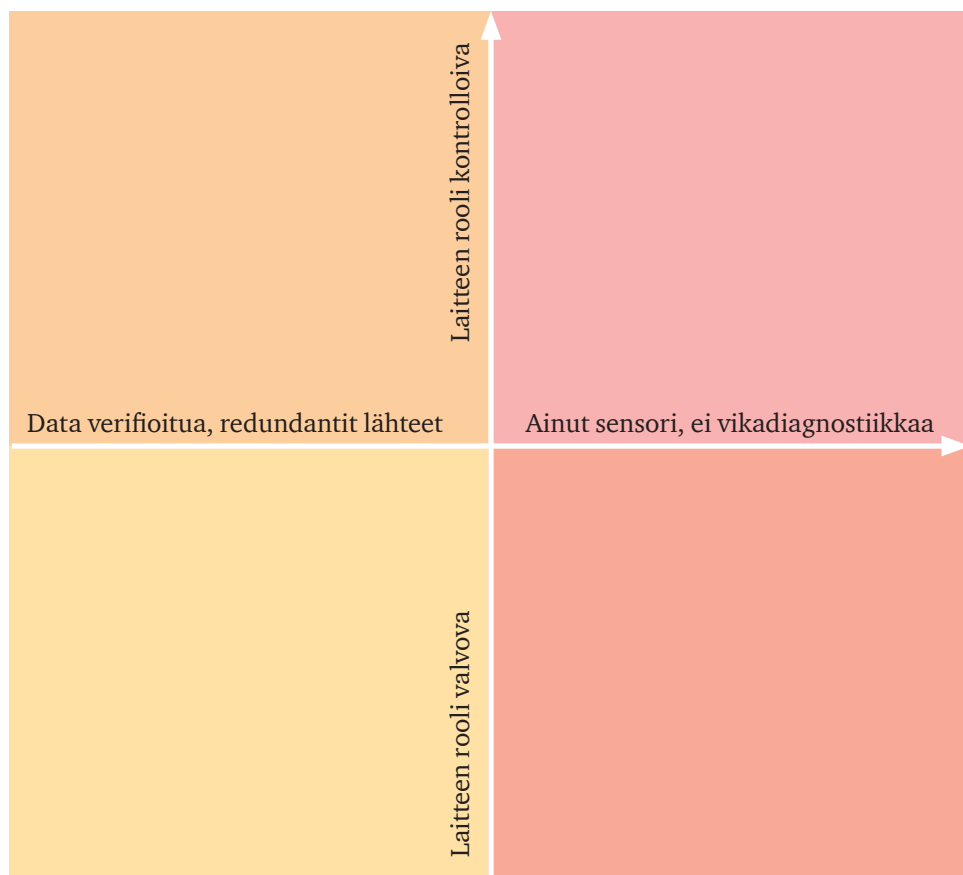
Laitteiden internetin uhkakuvat ovat tunnistettavissa hyvin pitkälle jo käytössä olevien uhkamallien ja uhka-analyysien avulla. IoT-infrastruktuurin ympäristön ja ominaisuuksien selvittämisen jälkeen on mahdollista keskittyä luottamuksen jatkuvuuden ylläpitämiseen. Suojaustason ja järjestelmän vaatimusten tulee olla asianmukaisesti linjassa kokonaisuuden kanssa.

IoT-järjestelmän ja sen antureiden suojaaminen tulee suhteuttaa laitteen

toimintaympäristöön. Luotetussa ympäristössä kevyempi sisäisen ja ulkoisen suojauksen taso voi olla riittävä. Vihamielisessä ympäristössä, jossa hyökkääjän on mahdollista päästä sensoriin tai IoT-laitteeseen käsiksi, suojausta tarvitaan aina. Suojausta ei kuitenkaan tule rakentaa niin, että se rajoittaa laitteen huoltoa esimerkiksi antureiden vioittuessa tai niin, että laitetta on mahdotonta päivittää joko liiketoiminnan kehittyessä tai haavoittuvuuksien ilmetessä.

Laitteen altistuessa vihamieliselle ympäristölle, missä sen fyysinen koskemattomuus on uhattuna, tullaan uusien ongelmien pariin. Mikäli laitteeseen on vihamielisellä taholla fyysinen pääsy, uhkamallin tulee lähteä siitä, että laitteen

Laitteen toiminnan kriittisyyden tunnistaminen



sisällä olevat PSK-avaimet ja muut luottamukselliset tiedot vuotavat. Tämä itsessään aiheuttaa uhkia IoT-infrastruktuuriverkolle ja luottamuksen säilyttämiselle. IoT-laitteet on syytä segmentoida verkkotasolla tiukasti pieniin osiin ja eriyttää laitteet omiin WLAN- sekä VLAN-verkkoihin muusta IT-infrasta. Ympäristön tulee kyetä havaitsemaan ja reagoimaan tai hälyttämään mikäli esimerkiksi verkkoon kytketään sinne kuulumattomia laitteita tai mikäli IoT-laitteen anturi lähettää virheellistä dataa.

Haasteellisissa ympäristöissä erilaiset teknologiat auttavat rakentamaan IoT-laitteiden luottamusta ja turvallisuutta. Ehdottoman tärkeää on varmistua

tällaisten laitteiden debug-liitännöiden irtikytkennästä sekä laitteiden hallinta-liittymien suojauksesta muilla kuin arvattavilla *admin/admin* -tunnuksilla. Suojaratkaisuihin esimerkiksi ARMin TrustZone tai erilaiset TPM-ratkaisut (Trusted Platform Module) yhdistettynä tietojen vahvaan salaukseen ja perinteesiin fyysisiin suojauskeinoin muodostavat pohjan turvalliselle IoT-ratkaisulle. Infrastruktuuritasolla esineiden internet vaatii myös uudenlaisia tai uudelleen kohdennettuja havainnointi- ja valvontaresursseja ympäristön hallintaan. Se vaatii myös ylläpidettyjä laiterekistereitä ja muita mekanisme, kuten verkon pääsynvalvontaa, joiden avulla ympäristöä voidaan ylläpitää turvallisesti.

Matka sensoreista pilveen ja päätelaitteeseen

Internet of Things ja pilvipalvelut nivoutuvat hyvin tiiviisti yhteen. Pilvipalveluiden toimiessa sovellusalueena koko toiminnalle tulee myös tämän alustan olla suojattu. Pilvialustoissa skaalautumista käytetään monesti perusteluna niiden käyttöönotolle, mutta tässä yhteydessä tulee muistaa erityisesti pääsynhallintaan ja hallintatunnuksiin liittyvät ongelmakohdat kun palveluja skaalataan kertaluokissa ylöspäin. On tärkeää, että yrityksellä on toimivat identiteetin- ja pääsynhallinnan järjestelmät (IAM) federaatioineen, joita vasten laajeneva infrastruktuuri voidaan helposti saattaa keskitetyn käyttäjätun-nushallinnan piiriin.

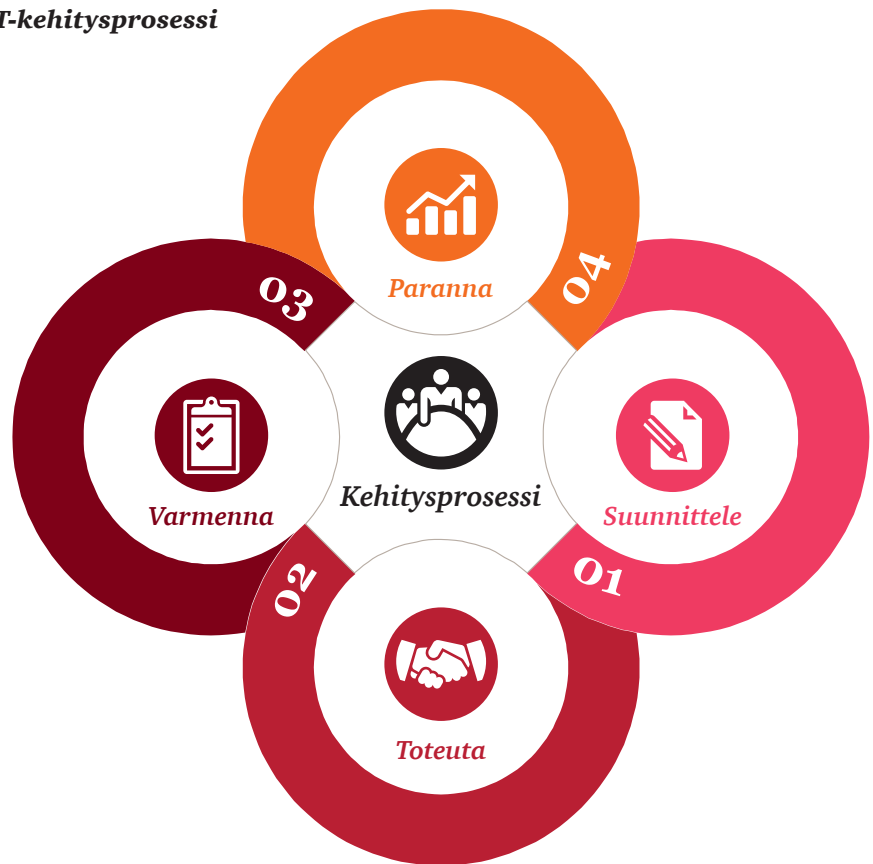
Liikenteen salaus IoT-laitteesta pilveen ja pilvestä mobiileihin päätelaitteisiin yhdistettynä pilvialustan suojauksella tekee esineiden internetistä luottamuksen näkökulmasta haasteellisen ympäristön. Tärkeintä järjestelmän määrittelyssä, ylläpidossa ja kehittämisessä on huolehtia koko ketjun turvallisuudesta.

Kuinka menestyä esineiden internetin kanssa

IoT tulee yleistymään, ja se on luontainen toimintaa edistävä kehityssuunta monilla aloilla. IoT tulee myös väijäämättä osaksi yritysten liiketoimintaa. Kun organisaatiot huomioivat esineiden internetiin liittyvät riskit ja haasteet sekä tiedostavat sen tuoman mahdollisuudet, IoT antaa vauhtia digitalisaatiolle ja luo lisäarvoa tehtailta asiakkaalle saakka.

IoT-ekosysteemit rakentuvat tyypillisesti toimittajien PaaS-tyyppisistä (Platform as a Service) ratkaisuksista, joissa on usein käytössä varsin paljon avoimen lähdekoodin ja avointen rajapintojen ratkaisuja joihin tilaaja harvoin voi suoraan vaikuttaa. Osaksi IoT-ekosysteemin kokonaisuutta tulee näin valitun IoT-toimittajan lisäksi muita toimijoita ja valmistajia, mikä nostaa ekosysteemiin kohdistuvia vaatimuksia monella eri tasolla.

IT-kehitysprosessi



Holistinen turvallisuusajattelu on paikallaan IoT-infrastruktuurien yhteydessä. Säilyttämällä luottamus kokonaisvaltaisesti läpi ketjun kaikkien lenkkien voidaan taata IoT-järjestelmän luotettavuus ja turvallisuus. Tietoturvallisuuden tulee viimeistään IoT:n kanssa integroitua osaksi normaalia IT:n kehityssykliä.

Luottamuksen takaaminen läpi ketjun voi vaikuttaa lähes mahdottomuudelta, mutta kokonaisuus nivoutuu kasaan hallitusti, kun asiaa tarkastellaan rauhallisen analyttisesti ilman suurta IoT-hypeä. Yrityksen IT-toiminnoissa aktiivisesti ylläpidetyt uhkamallit yhdistettynä luottamusmalleihin esineiden internetin parissa auttavat paikallistamaan järjestelmien heikkoja kohtia. Luottamusta vastaan hyökkääminen

altistaa IoT-infrastruktuurin haavoittuvuuksille, jolloin luottamuksen hallinta on ensisijaisen tärkeää sekä IT- että IoT-infrastruktuurin hallinnassa.

Esineiden internetin turvallinen käyttöönnotto ja käyttö edellyttävät perinteisen IT-riskienhallinnan osaamista sekä aktiivista otetta nopeasti kehittyvien ja laajenevien järjestelmien kehityksessä. Tärkeää on muistaa ottaa IoT aktiiviseksi osaksi yrityksen IT:n hallintasykliä ja pitää se mukana siellä niin, että IoT-laitteet pysyvät ajan tasalla ja kehittyvät asianmukaisesti prosesseissa koko elinkaariensa ajan. Jo normaalein riskienhallinnan keinoin esineiden internet saadaan otettua haltuun turvallisesti osaksi yrityksen arkista kehittyvää liiketoimintaa.

PwC:n kyber- ja IoT-asiantuntijat

Ota yhteyttä, niin keskustellaan lisää!



Karo Vallittu

020 787 8503

karo.vallittu@fi.pwc.com



Mikko Toivonen

020 787 8483

mikko.toivonen@fi.pwc.com



Marko

Hakkarainen

Tämä julkaisu on tarkoitettu yleisohjeistukseksi, eikä sitä voida pitää asiantuntijaneuvontaa vastaavana kannanottona. Lukijan ei pidä toimia tähän julkaisuun sisältyvän tiedon perusteella hankkimatta yksityiskohtaisempaa asiantuntijaneuvontaa. Emme takaa tähän julkaisuun sisältyvien tietojen oikeellisuutta tai täydellisyyttä, eikä PricewaterhouseCoopers Oy ota vastuuta niistä seurauksista, joita saattaa aiheutua lukijalle tai jollekin muulle taholle, mikäli he toimivat, ovat toimimatta tai tekevät päätöksiä tähän julkaisuun sisältyvän tiedon perusteella.

PwC:n kyberturvapalvelut

Haaste

Tietomurto!

Olenko turvassa?

Miten voisin suojautua?

Ammattitaitomme

Incident Response
Tunnista, rajaa vahingot, toivu

Tietoturvakvarmennus
*Varmennus, testaus,
varautuminen, koulutus*

**Turvallisuuden
kehittäminen**
Suunnittele, arvioi, toteuta

Lopputulema

**Vahingon ja tietovuodon
hallinta**

Liiketoimintavarmuus

**Turvallisuuden
tehostuminen**



PwC Suomi:



PricewaterhouseCoopers Oy, PL 1015 (Itämerentori 2), 00101 Helsinki. Puhelin 020 787 7000.

PwC auttaa yrityksiä kasvamaan, toimimaan tehokkaasti ja raportoimaan luotettavasti. Apunasi on Suomessa yli 830 asiantuntijaa ympäri maan. Palveluitamme ovat liikkeenjohdon konsultointi, yritysjärjestelypalvelut, veroneuvonta ja lakipalvelut sekä tilintarkastus- ja muut varmennuspalvelut. Tavoitteenamme on luoda kestävä kasvua. Ota yhteyttä tai lue lisää: www.pwc.fi.

PwC toimii 157 maassa yli 208 000 asiantuntijan voimin. Nimi PwC viittaa PwC-keijuun ja/tai yhteen tai useampaan sen jäsenyritykseen, joista jokainen on oma itsenäinen yhtiö. Lisää tietoa: www.pwc.com/structure.

© 2016 PricewaterhouseCoopers. Kaikki oikeudet pidätetään.