



Älykkäät järjestelmät

Alkuperäinen teksti (the original text):
Insurance Europe, Prevention Forum
Information for insurers, Smart Systems

Käännös (translation):
Suomen Pelastusalan Keskusjärjestö
The Finnish National Rescue Association

PALONTORJUNTATEKNIIKAN
kehitysryhmä



Sisältö

Tässä artikkelissa tutkitaan niin kutsuttujen älykkäiden järjestelmien nykyistä sukupolvea. Näihin järjestelmiin viitataan joissakin yhteyksissä termillä kotiautomaatio, vaikka kyseisiä järjestelmiä on alettu käyttää yhä enenevässä määrin yritystoiminnassa, erityisesti pienyritysten liiketiloissa. Kyseisillä järjestelmillä on monia eri tehtäviä, mutta tässä artikkelissa näitä järjestelmiä käsitellään vain tilojen turvallisuussovellusten merkityksessä. Muut sovellukset, kuten vesivuotojen havaitsemiseen, lämmityksen automaattiseen valvontaan sekä kaasun ja tulipalojen havaitsemiseen tarkoitetut sovellukset ovat vakuutusyhtiöiden kannalta tärkeitä ja jotkut tutkituista ongelmista vaikuttavat myös näihin toimintoihin.



Mikä on älykäs järjestelmä?

Älykkään järjestelmän ymmärretään yleisesti olevan verkosto, joka liittää toimitiloissa olevat älylaitteet toisiinsa. Vaikka älylaitteet voivat toimia myös itsenäisesti (kuten ohjelmoitava valokytin), tällaiset laitteet on yleensä tarkoitettu liitettäväksi (tavallisesti langattomaan) älykkääseen järjestelmään, jota ohjataan tavallisesti keskitetysti käyttöliittymän keskusyksikön kautta. Älylaitteella tarkoitetaan laitetta, joka toimii ainakin jollakin tasolla itsenäisesti ja joka kykenee yhdessä järjestelmän muiden laitteiden kanssa vastaamaan tai reagoimaan ympäristön tapahtumiin tavalla, joka tuo lisäarvoa käyttäjälle, joka ei voi saada kyseistä toimintaa aikaan yksittäisillä ”passiivisilla” laitteilla. Toisaalta on olemassa myös suunnittelufilosofioita, jotka perustuvat sille ajatukselle, että järjestelmän käytössä olevat laitteet ovat passiivisia ja itse järjestelmän älykkyys sijaitsee keskusyksikössä.

Suurin osa näistä laitteista saa tehonsa sisäänrakennetusta akusta. Yleisimpiä laitteita ovat multimedian, valaistuksen, lämpötilan, turvallisuuden, valvontakameroiden, kulunvalvonnan ja palontunnistuksen ohjaus- ja valvontalaitteet. Älykäs toiminto on esimerkiksi sitä, että järjestelmän ohjelmisto tallentaa anturijärjestelmältään saamia tietoja ja tekee tämän jälkeen jonkin ihmishajauksesta riippumattoman toiminnon, kuten valmistelee esimerkiksi omistajansa kotiintuloa säätämällä lämpötilaa, aktivoimalla valaistusta, avaamalla autotallin oven, käynnistämällä kotiviihdejärjestelmän jne. Jotkin järjestelmät voivat jopa avata ulko-oven, jos omistajan havaitaan olevan lähellä. Monet laitteet edellyttävät jonkinasteista alkuvuorovaikutusta, jotta niiden toiminnan voidaan katsoa olevan ”älykästä”. Käyttömukavuuden lisäksi näillä järjestelmillä voi olla myös energiaa säästävää vaikutus.

Muita mahdollisia ominaisuuksia voi olla esimerkiksi laitteiden hallinta kätevästi useammasta kuin yhdestä sijainnista tai etäyhteydellä Internet-yhteydessä olevalla älypuhelimella, tabletilla, tai tietokonepäätteeltä. Järjestelmän ja ”isäntäpalvelun” välillä voi olla myös käytössä verkkoyhteys tietojen keräämiseksi, päivitysten lähettämiseksi, pilvitalennustilan tarjoamiseksi ja/tai päätelaitteeseen liittämiseksi.

Keskusyksikkö on yleensä älykkään järjestelmän erillinen osa, jonka toiminta muistuttaa hyvin paljon turvajärjestelmien ohjaus- ja valvontalaitteiden toimintaa. Keskusyksikkö voisi yhtä hyvin olla yhdistettynä tuotteeseen, joka tavallisesti löytyy kotoa tai työpaikalta, mutta joka osallistuu järjestelmän toimintaan (ilmastoinnin ohjauslaite, televisiovastaanotin tai jopa jääkaappi).

Mitkä ovat mahdolliset ongelmat?

On tärkeää huomioida, että näitä tuotteita ja palveluita on kehitetty niin kutsutun esineiden Internetin (IoT) saralla. Tuotteilla olisi hankalaa päästä markkinoille perinteisten palontorjunta- ja turvallisuusjärjestelmien kautta. Vaikka niiden suunnittelijoilla näyttääkin olevat erittäin kehittyneet taidot "trendikkäiden" järjestelmien suunnitteluun, näihin taitoihin ei kuitenkaan näytä kuuluvan turvallisuusnäkökohtien huomioiminen.

Turvallisuuden ja yksityisyyden ollessa vaarassa sellaisia perusturvatoimia, jotka ovat perustavanlaatuisia muualla tietokone- ja verkkoaloilla, ei näytetä ymmärrettävän, niitä laiminlyödään tai niitä on toteutettu huonosti. Itse asiassa esineiden Internet perustuu ajatukseen, josta suunnittelijatkin saattavat olla tietoisia. Tämän ajatuksen mukaan miljoonien päivittäin käytettävien tuotteiden tulisi olla näkyviä toisilleen eikä sijaita kybersuojien takana, joiden tarkoituksena on eristää ne.

Lukuisat markkinatoimijat kilpailevat saadakseen tuotteensa markkinoille niin nopeasti kuin se vain on mahdollista lisätäkseen omaa markkinaosuuttaan. Turvallisuustuotteen suunnittelussa arvostetaan näennäisen vähän tuotteen turvallisuusperiaatteita, joista vähäisimpänä ei voida pitää täysin kehittyneen tietoturvalvannon tarvetta. Osa näiden tuotteiden myynti- ja markkinointimateriaalista voi olla harhaanjohtavaa esimerkiksi siltä osin, että tiedot välitettäisiin poliisille.

Älykkäiden järjestelmien markkinoilla, joissa toimijoina on tällä hetkellä Applen, Googlen ja Samsungin kaltaisia merkittäviä nimiä, on se, että nämä "raskaan sarjan" toimijat pyrkivät saamaan markkinoita omaksuma heidän omistuksessaan olevia käyttöprotokollia, minkä seurauksena kaikkien järjestelmässä olevien laitteiden on oltava yhteensopivia kyseisen protokollan kanssa. Myös yleishyödylliset yritykset (kuten kaasu- ja sähköyritykset jne.) ovat myös erityisen merkittävässä asemassa hyödynnettäessä tekniikkaa täysimääräisesti. Yrityksillä on valtavat resurssit ja verkostot toiminta-alueellaan. Koska älykkäille järjestelmille ei ole yhtä sovittua kansainvälistä tai teollisuudenalakohtaista standardia, markkinat ovat tässä kehitysvaiheessa hyvin hajanaiset yhteensopivuusongelmien takia.

Tämä yhteensopivuusongelma ulottuu lisäksi järjestelmän verkkoteknologiaan, joka saattaa hyödyntää perinteistä lyhyen kantaman tiedonsiirtoa, kuten paikallisverkkoa, Wi-Fi-tai Bluetooth-yhteyttä tai pientä joukkoa uusia, pienitehoisia verkkoja, jotka on kehitetty erityisestirajalliselle tietomäärälle, jota on vaihdettava älykkään järjestelmän komponenttien välillä. Tämä on siis yksi ongelma lisää mahdollisen yhteensopimattomuuden vyyhtiin.

Joissakin älykkäiden järjestelmien keskusyksiköissä käyttäjä tai asentaja voi liittää eri tuotemerkkien älylaitteita järjestelmään, jos ne ovat yhteensopivia paikallisen langattoman verkon ja keskuksen kanssa. Nämä niin kutsutut "avoimet ekosysteemit" muodostavat siten kilpailevat markkinat niille järjestelmille, joissa kaikki laitteet kuuluvat saman tuotemerkin piiriin. Mahdolliset vaikeudet saattavatkin johtua siitä, että koska älykkään järjestelmän kaikkia komponentteja ei ole suunniteltu yhteensopiviksi. Tällöin järjestelmän toiminnallisuus saattaa kärsiä tai siinä saattaa esiintyä tietoturvaluutteita.

Alan suunnittelijat pitävät erittäin tärkeänä käyttöönoton ja toiminnan yksinkertaisuutta (mutta usein jäävät tavoitteista). Tämä voi johtua suurelta osin heidän toiveestaan tehdä tuotteista sopivia ja houkuttelevia, esimerkiksi tee se itse (DIY) -ostajien tai sähkö- tai lämmitysjärjestelmiin suuntautuneisiin asennuksiin. Voi olla, että tietyt laitteet noudattavat tunnustettuja kansallisia tai kansainvälisiä standardeja, kuten EN 5013X -standardeja, mutta tällöinkin kyseessä on hyvin pieni vähemmistö.



Näin ollen, vaikka usein oletetaan, että hyväksytyt palontorjunta- ja turva-alan yritykset ovat asentaneet älykkäiden järjestelmien laitteita, maakohtaisesti tämä voi olla ristiriidassa alakohtaisen tarkastuskäytäntöjen ja ohjeiden kanssa, mikäli komponentit eivät ole sovellettavien palo-/turvallisuusstandardien mukaisia. Tästä seuraa mahdollisesti, että kyseiset järjestelmät eivät voi välttämättä saada vakuutusyhtiöiden hyväksyntää, jos vakuutusyhtiö edellyttää vakuutusturvan myöntämiseksi järjestelmää, joka vastaa palontorjunta-/turvallisuusstandardeja. Lisäksi ei-hyväksytyjen yritysten asentamat järjestelmät eivät todennäköisesti kuulu rutiinitarkastusten tai ehkäisevän huollon piiriin eikä turvallisuushenkilöstöä voida todennäköisesti kouluttaa asianmukaisesti.

Lisäksi kuitenkin älykkäiden järjestelmien valmistajat näkevät perinteisen palontorjunta- ja turvallisuusalan kohdemarkkinoinaan. Hämmäntävää kuitenkin sinänsä on, että jotkut älykkäiden järjestelmien palveluntarjoajat tarjoavat vastaavanlaisia hyvin tunnettujen hälytysten vastaanottokeskusten palveluja, joista aikaisemmin on tehty sopimuksia vain hyväksytyjen järjestelmien palveluntarjoajien kanssa. Tällöin on mahdollista, että vakuutusyhtiöitä johdetaan harhaan antamalla olettaa, että älykäs järjestelmä on täysin pätevä ja tunnustettujen standardien mukainen ainoastaan siksi, että se on yhdistettävissä sidosryhmien tuntemaan hälytysten vastaanottopalveluihin, jotka toimivat perinteisillä palontorjunta- ja turvallisuusjärjestelmämarkkinoilla.

Erityishuomautus

Vakuutusyhtiöiden ja muiden sidosryhmien ei tule sekoittaa tässä artikkelissa kuvattuja tuotteita viime aikoina käyttöönotettuihin älypuhelinsovelluksiin, joita valtavirtaan kuuluvat palontorjunta- ja turvajärjestelmiin erikoistuneet palveluntarjoajat ovat tuoneet markkinoille. Niiden avulla käyttäjä voi ohjata ja hallita järjestelmää Internetin kautta tarjottavalla etäyhteydellä, edellyttäen, että toimittaja voi osoittaa, että sovellus on suojattu riittävällä tavalla kyberhyökkäysten ja väärin hälytysten varalta. Tällöin vakuutusyhtiö voi hyväksyä tällaisen järjestelmätoiminnan muodon, joka tällä hetkellä kasvaa nopeasti käyttäjien keskuudessa. Yksi tapa, jolla järjestelmän tarjoaja voi vakuuttaa käyttäjän tai tämän vakuutusyhtiön siitä, ettei sovellus sisällä tietoturvaluutteita, on osoittaa todisteet asianmukaisuudesta. Tämä voidaan tehdä esimerkiksi tunnustetun testaus- ja sertifiointiorganisaation myöntämän suorituskykyvarmenteen avulla.

Erityiset turvallisuuskysymykset

Useissa eri tutkimuksissa ja raporteissa, joista jotkin ovat luotettavien organisaation laatimia, on löydetty laajoja turvallisuuspuutteita älykkäissä järjestelmissä.

Näistä esimerkkeinä ovat seuraavat:

- heikko, yksittäiseen tekijään perustuva todennus
- järjestelmät, joiden kautta murtautumalla päästään käsiksi videosuoratoistoon
- heikot salasanapalautusmekanismit
- epäonnistuneita kirjautumisyrittäjiä koskevan rajoituksen puuttuminen
- epäluotettavat pilvi- ja mobiilikäyttöliittymät
- perustavanlaatuiset puutteet turvallisuusasetuksissa
- turvallisuusasetukset vaarantava salauksen puute

Tilojen turvallisuuden etävalvonta muodostaa kuitenkin vakavan uhan turvallisuudelle, jos tilojen omistaja ei ole ainoa, joka tilaa valvoo.

Hakkereille altistuneiden laitteiden ja järjestelmien tietoturva-avoittuvuudet alkavat kiertää nopeasti väärillä verkkosivustoilla. Esimerkiksi joissakin sähköisissä lukoissa havaittuja haavoittuvuustietoja on jaettu laajasti. Hakkerin murtautumistarkoituksessa tilapäisesti hakkerioima lukko ei välttämättä anna omistajalle mitään vihjettä siitä, miten vahinko tapahtui.

Niinkin vähäpätöinen asia kuin termostaatin hakkerointi voi tarjota murtautujalle arvokasta tietoa esimerkiksi siitä, onko perhe kotona vai lomamatkalla. Jos suojaukset ovat helposti murrettavissa, hakkeri saa käyttöönsä valtavasti tietoa, kuten sen, onko ulko-ovi tai autotallin ovi lukittu jne. Myös henkilötiedot, luottokorttitiedot mukaan luettuna, voivat olla vaarassa. Laitte voi muodostaa Internet-yhteyden automaattisesti ilman, että omistaja ymmärtää täysin sen merkitystä. Käyttäjällä ei tavallisesti ole valtaa siihen, millaisia tietoja isäntäpalvelun käyttöön tarjotaan.

Sen lisäksi, että isäntäpalvelu voi kerätä keskusyksiköstä tietoja, sillä voi myös olla kyky hallita sitä tietyillä tavoilla. Lisäksi se saattaa voi olla este palvelun tarjoamiselle (esimerkiksi riitatapauksissa). Jos suojaus on riittämätön, hakkeri voi mahdollisesti kaapata nämä oikeudet. Ymmärrettävää on, että uusien kotitalouslaitteiden omistajat eivät yleensä määritä laitteen käyttäjätunnusta ja salasanaa verkossa, vaikka he ymmärtäisivätkin, miksi niin tehdään. Siksi ensimmäiset satoja tuhansia laitteita sisältävät bottiverkot, joissa botit pommittavat kohteitaan viesteillä sabotointitarkoituksissa, on jo havaittu.

Tulevaisuudennäkymät

Älykkäät järjestelmät vaikuttavat näennäisesti houkuttelevilta ja niitä tarjoavat yritykset ovat tavallisesti suuria ja taloudellisesti vahvoja yhtiöitä, joilla on kunnianhimoiset tavoitteet kyseisellä sektorilla. Perinteisten ja konservatiivisten yritysten innovaatio- ja markkinointiosastot, kuten yleishyödyllisten palvelujen tarjoajat, kansalliset verkko-operaattorit, kuluttajaelektronikan toimittajat ja vakuutusyhtiöt voivat nähdä älykkäiden tuotteiden osoittavan edistyksellistä lähestymistapaa teknologiaan ja innovatiivisiin kuluttajaetuihin. Yleisö on taipuvainen luottamaan kyseisiin instituutioihin mutta muuttuuko tämä käsitys, jos niiden johtajat eivät ymmärrä kuluttajille tästä aiheutuvia riskejä?

Hyödyntämällä kotiautomaatilaiteiden haavoittuvuuksia hyökkääjät voivat kerätä tietoa kohteistaan ja vaarantaa heidän omaisuuden, yksityisyyden ja turvallisuuden sekä tarkkailla samalla heidän käyttäytymismallejaan. Olisi ironista, jos älykkäitä turvallisuuslaitteita hankkineet joutuisivatkin siten alttiimmiksi rikoksille kuin jos he eivät olisi hankkineet mitään laitteita. Odotettavissa on kuitenkin, että vuoteen 2020 mennessä käytössä on noin 50 miljardia IoT-laitetta. Tällöin voidaan myös kerätä valtavia määriä tietoja väestön käyttäytymisestä.

Kaupallisella puolella yritykset ovat pitkään tunnustaneet taloudelliset edut, jotka liittyvät lämmitykseen, ilmanvaihtoon ja ilmastointiin rakennusten hallintajärjestelmissä. Palontorjunta ja turvallisuuden valvonta on yhdistetty näihin järjestelmiin jo useiden vuosien ajan. Tärkeimmät rakennushankkeet, olivatpa ne sitten suunniteltuja tai spekulatiivisia, todennäköisesti osoittavat, että älykäs rakennuksen hallinta on sisäänrakennettua. Onko olemassa vaara, että markkinoilla olevien kuluttajatuotteiden huono turvallisuus voi heikentää markkinoita? Ainakin uusia rakennuksia koskevia markkinastandardeja on olemassa ja niitä sovelletaan ainakin viestintäväylien osalta. Tällaisia standardeja ovat muun muassa kotien ja rakennusten elektroniikkajärjestelmiä koskeva EN 50090-standardi. Tällä välin älykkäät järjestelmät ovat alkaneet tunkeutua pienyrityssektorille.

Joidenkin vakuutusyhtiöiden uskotaan näkevän älykkäät järjestelmät sellaisina, että ne pystyvät parantamaan tuloksia paremman älykkyyden kautta. Kotitalouksiin keskittyvillä vakuutusyhtiöillä olisi mahdollisuus saada käyttöönsä suuri tietomääriä, joista ne voivat muodostaa hyvin tarkan kuvan liiketoiminnastaan ja asiakkaidensa käyttäytymisestä. Yksilötasolla voitaisiin seurata käyttöasteita ja vakuutuksenottajia voitaisiin palkita sen perusteella, lämmittävätkö he talojaan asianmukaisesti ja valvovatko he niiden kosteustasoja sekä turvallisuutta talojen ollessa tyhjiillään. Vakuutusyhtiöiden haasteena voi olla se, että voidakseen asettaa itsensä siihen asemaan, että ne voivat saada näitä tietoja, ne saattavatkin tahattomasti tukea sellaisten turvallisuusjärjestelmien käyttöönottoa, jotka muodostavat turvan sijasta turvallisuusriskin.

Lisäksi vakuutuksenottajia, joita nyt houkuttelee tai rohkaistaan ottamaan käyttöön älykkäitä järjestelmiä, on vaikea vakuuttaa asianmukaisen järjestelmän tarpeesta. Vakuutusyhtiöiden tuleekin seurata alan kehitystä. Markkinoiden kehittyessä, älykkäiden laitteiden alalla, tarvitaan vaikuttamista yhteisten käytänteiden käyttöönottamiseksi.

Suosituksset

Kunnes kotiautomaatiota ja älykkäitä järjestelmiä koskevat markkinat saadaan kestävämmällä pohjalle ja tunnustetuilla standardeilla suojatut turvallisuustuotteet erotellaan entistä selkeämmin, on varsin epätodennäköistä, että kotitalouksien ja pienyritysten pitäisi sallia olettaa, että nämä järjestelmät tarjoaisivat itseisarvona välttämättä hyvää turvallisuussuojausta. Vakuutusyhtiöiden tulisi harkita keinoja kertoa tästä hienovaraisesti asiakkailleen.



© Insurance Europe Prevention Forum
November 2017
All rights reserved

Publishing house: VdS Schadenverhütung GmbH Amsterdamer Str. 174 • D-50735 Cologne • Phone: +49 (0)221 / 77 66 - 0
• Fax: +49 (0)221 / 77 66 - 341

"Insurance Europe Prevention Forum's Information for insurers — Smart systems, November 2017" is subject to copyright with all rights reserved. Reproduction in part is permitted if the source reference "Insurance Europe Prevention Forum, Information for insurers — Smart systems, November 2017" is indicated. Courtesy copies are appreciated. Reproduction, distribution, transmission or sale of this publication as a whole is prohibited without the prior authorisation of the Insurance Europe Prevention Forum.

Although all the information used in this publication was taken carefully from reliable sources, Insurance Europe and the Insurance Europe Prevention Forum do not accept any responsibility for the accuracy or the comprehensiveness of the information given. The information provided is for information purposes only and in no event shall Insurance Europe or the Insurance Europe Prevention Forum be liable for any loss or damage arising from the use of this information.