

Bristande säkerhet hot mot smarta städer

<https://fastighetssverige.se/artikel/bristande-sakerhet-hot-mot-smarta-stader-26704>

Publicerad den 7 December 2017

Teknik År 2020 kommer det att finnas över 20 miljarder ”smarta” och uppkopplade objekt enligt Gartner. Det ställer stora krav på säkerheten, trots det väljer många företag som hjälper till att bygga upp smarta städer att prioritera bort det i sina strategier. Mer än varannat företag har även stora utmaningar att få till ett system som är säkert, det visar en ny undersökning som Vanson Bourne gjort på uppdrag av den icke-vinstdrivande branschorganisationen Wi-Sun Alliance.

Framtidens städer blir alltmer uppkopplade och med digitaliseringens framfart, alltifrån att än fler applikationer, komponenter, tjänster och sensorer kopplas på, följer en mängd digitala säkerhetshot. Det ställer högre krav på hur säkerheten ska utformas för smarta städer och andra IOT-system. – Det är inte längre bara datorer, mobiler eller uppkopplade prylar som skrivare som ligger i farozonen för cyberattacker. När alla prylar kopplas upp mot Internet kan den vanliga infrastrukturen i en stad bli en svag länk för cyberhot. Tyvärr finns det alltid cyberkriminella som vill utnyttja svagheter för att tjäna pengar eller sabotera på andra sätt, säger Phil Beecher, ordförande och vd för Wi-Sun Alliance. Undersökningen från Vanson Bourne, på uppdrag av Wi-Sun Alliance, visar att endast 49 procent av respondenterna från de svenska företagen, som för närvarande arbetar med IOT-initiativ, har tagit med i strategin hur de ska skydda IOT-systemen mot cyberattacker. Den visar också att 54 procent av respondenterna anser att den största tekniska utmaningen är att få till ett säkert system, följt av att hitta arbetskraft som kan jobba med IOT (48 procent) och interoperabilitet (46 procent), dvs att olika enheter och sensor kan kommunicera med varandra på ett bra sätt. – Problemet är bland annat att utvecklare på området ”smarta städer” oftast fokuserar på funktionerna i första hand och inte säkerheten. Det innebär att flera olika system skapas som blir enklare att hacka vilket kan leda till katastrofala följder som inte bara hotar vanliga människor, utan även industrier, infrastruktur, näringsliv och viktiga samhällsfunktioner. Därför är det viktigt att få till en gemensam lösning för att få till ett kompatibelt, säkert och pålitligt system som använder sig av öppna standarder, säger Phil Beecher. Undersökningen visar också att: # 38 procent av respondenterna i de svenska företagen, som för närvarande arbetar med IOT, har stött på säkerhetsproblem när de försökt att implementera IOT-lösningar. # Nästan hälften (44 procent) av respondenterna i de svenska företagen, som för närvarande investerar i IOT, har en fullt implementerad IOT-plan. # 87 procent ansåg att de har varit svårt att implementera en IOT-plan. # 98 procent av de tillfrågade respondenterna i de svenska företagen anser att de måste investera i IOT inom tolv månader för att fortsatt vara konkurrenskraftig.

- Axel Ohlsson

axel@fastighetssverige.se