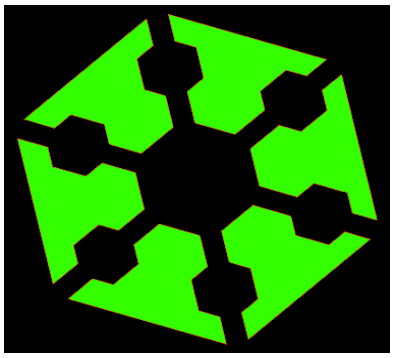
Sikkerhed og privatlivsbeskyttelse i en ”smart” storby – et oplæg

Arbejdsgruppen for borgerdrevet innovation og Open Everything

v/ Open Space Aarhus, http://osaa.dk



En moderne by, hvor der overalt er implementeret digital teknologi med henblik på en optimering af borgernes kommunikation og byens processer - en *smart city* - er udstyret med millioner af sensorer, der til hver en tid indsamler store mængder af data. Disse data kan indsamles og analyseres, og en sådan omfattende *data mining* kan give en indsigt i byens processer, der kan give helt nye muligheder for at planlægge, så byen fungerer bedre i miljømæssig, energimæssig og økonomisk henseende.

Denne forbedrede planlægning kan spare penge og energi og gøre det nemmere for borgerne at bevæge sig rundt i byen, og det kan i sidste ende føre til en langt mere velfungerende by med mere livskvalitet for borgerne. Mange af disse anvendelser er skitseret i Alexandra Instituttets oplæg om "The Internet of Things" (http://www.theinternetofthings.eu/content/mirko-presser-iot-comic-book).

Tilstedeværelsen af disse mange sensorer og generelt af den megen IT på alle niveauer medfører dog også en større risiko. Dårligt designede løsninger kan kompromittere borgernes sikkerhed og privatliv på nye og uforudsete måder. Dette kan føre til forringelse af borgernes livskvalitet, men der er også en risiko for, at sikkerhedsmæssige problemer med ny teknologi får borgerne eller statslige kontrolorganer til at forkaste en ellers velfungerende løsning - hvilket kan medføre store omkostninger til genanskaffelse. Den slags problemer skyldes oftest, at teknologien er for kompleks, til at det er muligt at overskue de sikkerhedsmæssige konsekvenser af en beslutning, hvis man ikke er ekspert på området. Det er derfor vigtigt at indtænke sikkerhed og privatliv i alle faser af enhver af de nye og "smarte" teknologier, hvis ikke man skal risikere en række meget ubehagelige overraskelser.

Som et eksempel kan vi forestille os en moderne bolig udstyret med såkaldte "smarte målere", der kortlægger husstandens el-, vand- og varmeforbrug. Sådanne sensorer kan måle ikke blot mængden af energi, der bliver forbrugt, men også detaljerne - tidspunkt, placering i huset, forholdet mellem husstandens forskellige elektricitetsforbrugende apparater.

Med den slags detaljerede målinger kan det blive nemmere for forsyningsselskabet at forstå og dermed planlægge, hvornår forbruget er "roligt", og hvornår de kan forvente at se "peaks", som de er nødt til at have kapacitet til. En analyse af data fra den enkelte husstand kan bruges til at optimere husstandens energiforbrug og kan spare den enkelte forbruger for betragtelige beløb på el- og varmeregningen.

Indsamlingen af så detaljerede oplysninger om den enkelte husstands forbrug giver dog alvorlige problemer netop i forhold til husstandens sikkerhed og privatliv. Det er vigtigt at få afgrænset, hvor detaljerede oplysninger forsyningsselskabet skal modtage, og

hvad det skal kunne gøre med dem. Er det forpligtet til at opbevare dem, skal det kunne udlevere dem til samarbejdspartnere i andre myndigheder, og skal det ligefrem kunne sælge dem til andre private firmaer? Skal det i yderste konsekvens offentliggøre dem?

Hvis en husstands forbrug af el og vand synker til noget nær ingenting i en periode, er familien givetvis ude at rejse. Hvis en enlig sjældent har noget forbrug om aftenen og om natten, sover vedkommende måske andetsteds og sammen med en partner. Hvis en husstand ofte er ude at rejse, vil den regelmæssigt have perioder med et meget lavt forbrug. Hvis strømforbruget altid vokser med ca. 100 watt i 50 minutter hver tirsdag, ser familiens medlemmer nok en bestemt krimi, der går om tirsdagen.

Alle disse oplysninger er relevante, når man skal beregne den helt optimale indstilling for husstandens el- og varmeapparater såvel som for forsyningsselskabets planlægning for byens forskellige kvarterer. De kan imidlertid også bruges til andre ting. En liste over familier, der er ude at rejse i længere tid, er en guldgrube for indbrudstyve. Hvis en person ikke sover i sit eget hjem, sover vedkommende måske hos en tidligere partner - og det kan være af interesse for kommunens socialforvaltning. Hvis en familie ofte er ude at rejse, kan de have gavn af målrettede tilbud om charter-rejser og "frequent flyer"-rabatter. Og hvis husstanden altid ser en bestemt krimiserie, vil de måske være interesseret i et godt tilbud på DVD-udgaven. Der kan drages meget vidtgående konklusioner ud fra sådanne data: Hvis en husstand pludselig begynder at bruge elektricitet sidst på aftenen i to værelser i stedet for ét, ligger det mangeårige ægtepar sandsynligvis i skilsmisseforhandlinger og bør have tilsendt en brochure fra kommunen, der tilbyder vejledning i denne svære situation.

Disse ”afledte” oplysninger er *helt irrelevante* for det spørgsmål, som de smarte sensorer egentlig skal hjælpe med at afklare, nemlig husets energiforbrug. Når data først er indsamlet, hvem skal så eje dem, og hvem skal have ret til at se dem? Det siger sig selv, at indbrudstyve ikke skal have adgang til at lave en liste over husstande, der ikke har haft forbrug i en uge. Det er dog slet ikke utænkeligt, at kommunen på et tidspunkt vil forlange en liste over fraskilte mænd, der sjældent har forbrug om aftenen og om natten. Og oplysninger om forbrugsmønstre kan som demonstreret være særdeles interessante med henblik på målrettet reklame - hvilket også kan give forsyningsselskabet ekstra indtægter.

Mange mennesker vil dog mene, at indsamling af så detaljerede oplysninger om deres personlige forhold krænker deres privatliv og alene derved forringer deres livskvalitet. De ønsker ikke at modtage målrettede reklamer, fordi private firmaer har indblik i, hvornår de tænder for fjernsynet, og de ønsker heller ikke at modtage underlige opringninger fra kommunen, fordi de har fået natarbejde. Meget af dette er der allerede taget højde for i vores nuværende lovgivning, og Datatilsynet ville formentlig omgående standse planerne om en central database over detaljerne i den enkelte husstands forbrug, der kan deles med samarbejdspartnere.

Dette ændrer dog ikke ved, at et hus udstyret med sådanne smarte sensorer kan hjælpe husstanden med at ændre forbrugsmønster og spare penge. Det gælder altså om at finde et bæredygtigt princip for, hvem der ejer de data, der indsamles, og hvad der skal ske med dem.

Et simpelt og bæredygtigt princip, der passer godt til et åbent samfund, som det nye og smarte Aarhus ønsker at være, kunne være, at den enkelte - det være sig borger, husstand eller virksomhed - som udgangspunkt altid selv ejer sine data og selv bestemmer, hvem de skal deles med.

I vores eksempel vil det betyde, at eftersom forbruget er noget, som borgeren køber af forsyningsselskabet, må de helt detaljerede oplysninger om forbruget også tilhøre

borgeren selv. Husets smarte sensorer bør altså som udgangspunkt opsamles og behandles på en computer i selve husstanden, og kun de oplysninger sendes videre til forsyningsselskabet, som er relevante for afregningen. Denne computer bør hele tiden være under husstandens (og altså ikke forsyningsselskabets) fulde kontrol.

Dette vil ikke løse alle problemer ved en sådan "smart" registrering af husstandens forbrug, og formålet med dette eksempel er heller ikke at foreslå en løsning, men at vise, hvor store problemer, der potentielt kan opstå i selv den simpleste anvendelse af den nye teknologi.

Der findes mange eksempler på store IT-løsninger, der er rullet ud til borgerne og efterfølgende har vist sig at have store problemer, fordi sikkerhed og privatlivsbeskyttelse ikke var tænkt ind i dem fra starten. Vi kan nævne et par eksempler:

NemID er gjort kompatibel med Danske Banks gamle netbankslogin, men dens design bryder så voldsomt med grundlæggende principper for digital signatur, at det helt unødvendigt muliggør phishing-angreb, som vi så i efteråret 2011. Samtidig kompromitterer NemID potentielt (givetvis ikke reelt) borgernes privatliv, idet den kræver, at man installerer en såkaldt Java-applet, som får ret til at læse den enkelte brugers filer.

Rejsekortet A/S har ikke orden i sikkerheden i den forstand, at teknologien i selve kortet er forældet og kan hackes. Samtidig planlægger man af hensyn til afregningen at opbygge en central database over tid og sted for danskernes brug af offentlig transport. Hvis en sådan database blev kompromitteret og for eksempel gjort tilgængelig for kriminelle, kunne det få katastrofale konsekvenser for den enkelte borgers sikkerhed.

Rejsekortet og NemID er eksempler på, at man ikke har tænkt sikkerheden ind i projektet fra starten og derfor er endt med nogle meget dårlige løsninger, som medfører lapperi og i værste fald forsinkelser og udvikling af helt nye systemer - med spild af milliarder af kroner til følge.

Som en del af "Smart Aarhus" kunne Aarhus faktisk overveje selv at udvikle alternativer i form af en "Smart ID" eller et "Smart Buskort" som kan installeres på de mest udbredte smartphones og give adgang til busrejser og kommunale hjemmesider - men som i modsætning til Rejsekortet og NemID brugte den nyeste krypteringsteknologi til at løse problemet *uden* de grundlæggende problemer, der desværre ligger i Rejsekortet og NemID. Et "smart klippekort" kunne for eksempel implementere en slags kryptografisk poletsystem, så det stadig er muligt at rejse anonymt med bus og alligevel blot kunne fremvise en app på en smartphone, når kontrolløren kommer.

Den vigtigste pointe er dog, at de sikkerhedsmæssige problemer aldrig vil kunne løses til bunds. Den bedste løsning er at tænke sikkerheden og databeskyttelsen ind fra starten i hver eneste løsning, der udrulles. Man bør altid huske, at alle data potentielt kan kompromitteres - og det er derfor smart at indrette sine databaser og kommunikationslinjer, så konsekvenserne af en kompromittering bliver så små som mulige.

En metode til at sikre, at sikkerheden og en passende beskyttelse af borgernes privatliv altid tænkes med i kommunens IT-infrastruktur kunne være at udnævne en kommunal "sikkerhedsombudsmand". En person, der på baggrund af en solid indsigt i sikkerhedsproblemer ved moderne IT-løsninger kan fungere som "virtuel borger", vil kunne påpege problemer, som almindelige borgere ikke burde acceptere, hvis de kendte konsekvenserne. Ved at indføre en sådan ombudsmand kunne kommunen tage mange af de værste sikkerhedsmæssige problemer i opløbet, før de skal repareres og begynder

at koste penge - eller i værste fald skal kasseres.

En sikkerhedsombudsmand bør også være ekspert i de retslige og ikke mindst borgerrettighedsmæssige konsekvenser af den digitale teknologi, så det på forhånd sikres, at de løsninger, der indføres, er gangbare også i et åbent og demokratisk retssamfund. På den måde undgås det, at kommunen og dens samarbejdspartnere skal spilde tiden med berettiget kritik fra bekymrede pressionsgrupper, som vi for eksempel har set i forbindelse med den nye handelskonvention ACTA, hvor nogle enkelte problematiske afsnit har ført til politiske protester, der har forhalet processen meget betydeligt. Hvis man fra starten tager højde for borgernes berettigede indvendinger mod konsekvenserne for deres sikkerhed og privatliv, vil sådanne protester aldrig opstå og vil aldrig true processen - og samtidig sikres det, at Aarhus også som "smart city" kan forblive et frit og åbent samfund, som det kan være attraktivt for borgerne at bo i. I det globale marked vil det også være et plus i konkurrencen om at tiltrække den bedst kvalificerede arbejdskraft, for hvem muligheden for et friere liv kan give Aarhus en fordel frem for tilsvarende højteknologiske storbyer i andre dele af verden.

Skrevet af Carsten Agger, Magenta ApS

http://www.magenta-aps.dk