Region Hovedstaden

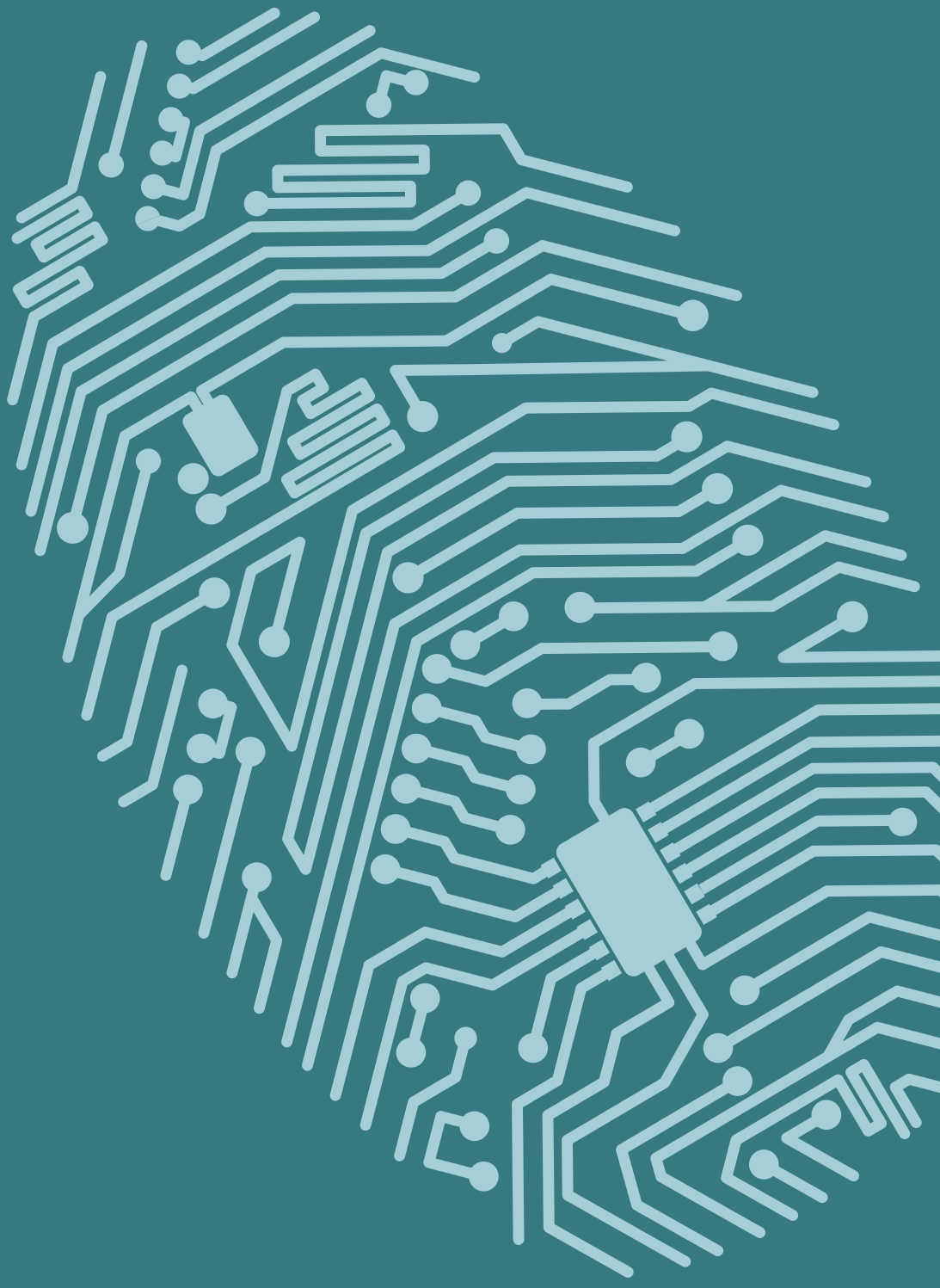
SMART CITY CYBERSECURITY LAB
SCL

// Håndbog i
smart city sikkerhed

Et dialogværktøj til kommuner og virksomheder

/ Håndbog i smart city sikkerhed /

Et dialogværktøj til kommuner og virksomheder



Partnerne bag Smart City Cybersecurity Lab er:

Udgivelsen af denne håndbog i smart city sikkerhed er gjort mulig af midler fra Region Hovedstaden til projektet Safer Copenhagen. Tilrettelæggelse og redaktion er forestået af Smart City Cybersecurity Lab (SCL). Udbredelsen af håndbogen sker i samarbejde med det fællesoffentlige Smart City Partnerskab med Danske Regioner, Digitaliseringsstyrelsen, Erhvervsstyrelsen, KL og Styrelsen for Dataforsyning og Effektivisering.

Redaktionsgruppe:
Marie Gottlieb Danneskiold-Samsøe, centerchef, Vallensbæk Kommune (formand).
Jette Sørensen, organisationskonsulent, Vallensbæk Kommune.
Christian D. Jensen, lektor, leder af sektionen for cybersikkerhed, DTU Compute.
Sam Afzal-Houshmand, forskningsassistent, DTU Compute.
Morten Andersen, forskningsjournalist, manjourn.dk.
Anders Pall Skött, senior forretningsudvikler, DTU (Sekretariatschef Smart City Cybersecurity Lab).

Spørgsmål om indholdet kan stiles til Anders Pall Skött: anps@dtu.dk, tlf.: 93 51 17 43.
Kontakt i Region Hovedstaden er Henrik Aagaard Johanson: henrik.johanson@regionh.dk, tlf.: 27 12 42 21.

https://www.sc-lab.dk/

ISBN nr.: 978-87-971357-1-6
1. udgave. December 2019.

Grafisk design og opsætning: Maja Pode Blarke, freelance grafisk designer. https://majablarke.myportfolio.com
Tryk: Baur Offset A/S.

/ Forord /

Interessen for smart city-løsninger er markant stigende i takt med, at kommuner og andre aktører finder løsninger, der kan spare på de offentlige udgifter eller give bedre løsninger inden for blandt andet miljø, klima, trafik og bygningsstyring.
I smart cities spiller privacy og cybersikkerhed en afgørende rolle, hvis vi skal bevare tilgængelighed, integritet og tillid fra borgerne. Formålet med denne håndbog er at give konkrete råd og vejledning til, hvordan kommuner og virksomheder kan håndtere sikkerheden. Samtidig skal den fungere som et dialogværktøj, der hjælper med at stille de rette spørgsmål og give eksempler på, hvad andre har gjort.

Målgruppen for håndbogen er offentlige indkøbere og leverandører samt andre medarbejdere, som har interesse i smart city løsninger uden at være specialister i sikkerhed. Forhåbentlig kan flere, for eksempel kommunalpolitikere, også få glæde af den.

Håndbogens indledende kapitel kridter banen op. Hvordan er smart city systemer opbygget, og hvilke trusler er de mest relevante at gardere sig mod?

Dernæst følger en beskrivelse af processen trin for trin ved etablering af et smart city system med fokus på, hvor det er vigtigt at tænke sikkerhed ind. Beskrivelsen rummer blandt andet de syv vigtigste punkter inden for sikkerhed, som bør indgå i kravsspecifikationen ved et smart city projekt. Desuden en guide til sikkerhedsanalyse.

Videre har vi skrevet et kapitel om sikkerhedsrisici og løsninger i forbindelse med det såkaldte LoRaWAN-system, som en række kommuner har valgt at basere deres smart city løsninger på. Hovedparten af de nævnte risici og løsninger er generelle. Dermed er kapitlet også anvendeligt for kommuner, der baserer sig på andre systemer, fx NB-IoT eller SigFox.

Desuden har vi skrevet et kapitel om forhold, der ligger rundt om selve sikkerheden. Økonomi er naturligvis altid en faktor i forbindelse med offentlige projekter. Samtidig kan der være menneskelige faktorer at tage hensyn til. En sikkerhedsløsning skal ikke kun fungere i udgangspunktet, men også under drift flere år frem i tiden.

For de læsere, der ønsker at gå et spadestik dybere ned i den tekniske baggrund omkring trusler og løsninger inden for smart city sikkerhed, har vi udarbejdet en teknisk sektion.

Endelig supplerer vi med en række cases og interviews, der viser, hvordan sikkerheden er tacklet i eksisterende smart city projekter.

God læsning!

Marie Gottlieb Danneskiold-Samsøe
Centerchef, Vallensbæk Kommune
Formand for Smart City Cybersecurity Lab (SCL)

/ Indhold /

/ Sammenfatning /

Denne håndbog har til formål at højne sikkerheden i smart city projekter. Fokus er især på hvornår i processen, det er vigtigt at tænke sikkerhed ind.

I komprimeret form lyder rådene på de forskellige trin i etableringen af et smart city projekt:

// Start dit projekt med at orientere dig i de lokale rammer for at køre et teknologi-projekt med fokus på sikkerhed. Find herunder ud af, hvilke vidanspersoner i organisationen, du kan trække på.

// Gør dig klart, inden du begynder at snakke med leverandører, hvilket formål dit system skal opfylde og, hvad det betyder for sikkerhed i løsningen.

// Foretag sikkerhedsanalyse (kortlæg angrebsflader og forebyggende foranstaltninger), foretag risikovurdering, få styr på relevant lovgivning og vær opmærksom på særlige forhold omkring brug af persondata.

// Din kravsspecifikation bør indeholde syv punkter om sikkerhed. Bed leverandøren specificere, hvordan hvert punkt tænkes opfyldt. Svarene giver ikke nødvendigvis mening for dig, hvis du ikke selv er ekspert i sikkerhed, men de sætter dig i stand til at indhente en "second opinion".

De syv punkter er: Hemmeligholdelse. Beskyttelse mod ændringer. Tydelig kilde til data. Retten til at teste. Overholdelse af standarder. Sletning af data og kassation af udstyr. Styr på opdateringer.

// Gå i dialog med leverandøren. Stå fast på, at du vil have ret til at teste sikkerheden og, at kommunen ejer data, og at du vil have mulighed for at tilgå rå-data.

// Sørg for tidligt at få afklaret opgaver og ansvarsforhold i drift-situationen. Hav en exit-strategi.

Rådene er uddybet i håndbogens kapitel "Smart city sikkerhed trin for trin".


8A Friheden St.
Hi-Fi klubben

/ Nye digitale muligheder, nye risici /

Kunsten er at udnytte smart city løsninger til at give borgerne bedre service og spare på ressourcerne – uden at åbne en ladeport for misbrug og læk af data.

Enhver Hollywood-thriller har en scene, hvor en af skurkene – altid ham med brillerne – hacker sig ind i en storbys infrastruktur. Snart er hele bydele mørklagte, eller der bryder kaos ud i trafikken, når signalerne skifter uforudsigeligt mellem rødt og grønt.

I praksis er det noget sværere at udføre den slags angreb, end det tager sig ud på film. Men i takt med, at kommunerne udnytter de nye digitale muligheder i form af smart city løsninger, bliver det stadig mere relevant at sikre sig.

I udgangspunktet må man erkende, at der ikke findes 100 pct. sikre systemer. Indsatsen omkring sikkerhed i smart city løsninger skal derfor koncentrere sig om at holde risici på et acceptabelt niveau. Det overordnede hensyn må være, at sikkerheden skal være så god, og de mulige skadevirkninger så små, at kommuner og de øvrige aktører ikke forhindres i at høste de mange gevinster ved vellykket digitalisering: bedre service til borgerne, lavere klimaaftryk af aktiviteterne, afskaffelse af overflødige arbejdsgange mv.

Med andre ord er det to forskellige opgaver, der skal løses. Den første er, at systemerne skal designes sådan, at risici minimeres. Den anden, at skadevirkningerne ved indtrængen i systemerne skal begrænses, så normaltilstanden hurtigst muligt kan genoprettes.

Dimser taler med hinanden via smalbånd

Alle prognoser viser, at der snart vil være flere maskiner end mennesker, som kommunikerer med hinanden. Et eksempel fra smart city universet er den kommunale skraldespand, der selv "ringer hjem", når den trænger til at blive tømt. Et andet eksempel er sensorer, som registrerer ledige parkeringspladser, hvorefter informationen automatisk bliver overført til digitale tavler, så bilisterne kan orientere sig, når de kører ind i bymidten.

Grundlæggende bygger sådanne anvendelser på IoT, altså Internet-of-Things. Der er ikke noget etableret dansk udtryk for IoT. Måske dimsernes internet?

Der er ligheder mellem menneskenes og dimsernes internet, men der er også forskelle.

Mange smart city anvendelser bygger på enheder, der sidder langt fra hinanden – og langt fra rådhuset. Det ville være alt for dyrt og besværligt at forbinde dem til systemet ved hjælp af de løsninger, som vi kender fra menneskets internet. Det vil sige en kombination af faste forbindelser samt lokale trådløse forbindelser som WiFi.

Smart city løsninger kan altså ikke udnytte den eksisterende infrastruktur for internettet. Men det er ikke nødvendigvis en dårlig nyhed. Gennem de seneste mange år er menneskets anvendelse af internettet blevet stadig mere domineret af underholdning. Overførsel af lyd og video kræver evne til at transmittere store datamængder hurtigt. Derfor har vi været nødt til at opgradere vores kommunikationsnetværk. I teknisk jargon har vi indført bredbåndsløsninger.

Det typiske smart city system har ikke brug for at overføre store mængder data i høj hastighed. Informationen om, at skraldespanden er fuld, kan gives som en simpel besked, og det meste af tiden er der slet ikke behov for kommunikation med enheden. Derfor kan man tillade sig at bygge smart city systemerne på helt andre løsninger. Man behøver ikke længere bredbånd. Og når man kan nøjes med smalbånd, er der mange penge at spare.

Større rækkevidde, lavere energiforbrug

Smalbåndsløsninger handler dog ikke kun om bedre økonomi. Når man sætter kravene ned til datamængder og hastigheder, åbner det for løsninger med væsentligt større rækkevidde. Dermed er det muligt at nå selv de fjerneste hjørner af kommunen.

Samtidig løser smalbånd et andet meget væsentligt problem. Alle elektroniske enheder har behov for strømforsyning, og desværre er der sjældent en stikkontakt ved hånden ude i byrummet. Derfor skal enhederne køre på batteri. Forestiller man sig, at enhederne skulle kommunikere over det almindelige mobilnetværk – 4G, snart 5G – ville batteriet hurtigt gå dødt. Med smalbånd kan batteriet holde meget længe forudsat, at der kun er tale om at overføre små mængder af data.

Kompatibelt smalbånd giver synergi

Hvordan sikkerheden i smart city systemet bør designes, afhænger i høj grad af, hvilket konkret formål systemet skal tjene. Desuden har det betydning, om systemet skal spille sammen med andre systemer i kommunen. Generelt er det ønskeligt, at det enkelte smart city system er kompatibelt med andre løsninger, fordi man så har mulighed for at høste ekstra gevinster af digitaliseringen. Men samtidig bliver det endnu mere vigtigt at sikre sig mod indtrængen, fordi skadevirkningerne så kan blive forstærket.

Yderligere et forhold, som har betydning for det konkrete valg af sikkerhedsløsninger, er, hvilken af de forskellige mulige smalbåndsløsninger, det pågældende smart city system hviler på.

I betragtning af forudsigelserne om eksplosiv vækst i dimsernes internet er det ikke overraskende, at en række udbydere konkurrerer om markedet for smalbånd. Vi gennemgår her kort de vigtigste (uddybes senere i håndbogen).

Tre gange smalbånd bejler til kunderne

I Danmark er der især tre smalbånds-løsninger på banen.

LoRaWAN (Long Range Wide Area Network) er udviklet af foreningen LoRa Alliance, der har over 500 virksomheder og organisationer i mange lande som partnere. LoRa er Open Source. Det vil sige, at alle kan bygge deres eget LoRa-netværk. For eksempel kan en kommune etablere et LoRa-netværk, der dækker hele kommunens område. Det udelukker ikke, at andre kan etablere et mere lokalt LoRa-netværk, der for eksempel dækker en enkelt virksomhed i kommunen. Nogle danske kommuner driver selv LoRa-netværk, mens andre har købt brug af LoRa-netværk som en service hos eksterne leverandører.

NarrowBand Internet-of-Things (NB-IoT) er skabt af en række teleselskaber. I sin funktion minder NB-IoT om LoRaWAN. En af forskellene er, at NB-IoT benytter sendefrekvenser, som kun teleselskaberne har lov til at benytte. Systemet sender via mobilnetværket, som teleselskaberne i forvejen driver. Blandt andet udbyder 3, TDC, Telia og Telenor smalbåndsløsninger baseret på NB-IoT. Som kommune vil man typisk tegne et antal abonnementer, et for hvert apparat i et smart city system. Apparaterne forsynes med hver deres SIM-kort.

SigFox er udviklet af den franske virksomhed med samme navn. Siden oprettelsen i 2009 er SigFox gradvist udbredt til stadig flere lande. I hvert land er der en bestemt operatør, som har eneret på SigFox. I Danmark er det virksomheden IoT Denmark, som introducerede sin første smalbåndsløsning i 2017 og siden har oplevet hastig vækst. En kommune, der ønsker at basere et smart city system på SigFox, bliver kunde hos IoT Denmark. Der tegnes et abonnement for hver enhed.

Desuden benytter en del smart city systemer WiFi blandt i situationer, hvor der i forvejen er etableret WiFi for det pågældende område. Desuden benytter mange systemer telefonnettet/GSM via indbyggede SIM-kort. Disse løsninger er ofte lette at sætte op, men dyre i stordrift-skala på grund af udgifterne til SIM-kort og abonnementer.

Lovpligtigt at beskytte personoplysninger

Det er vigtigt at skelne mellem to former for problemstillinger. Angreb på infrastrukturen med kriminelle formål eller for at udløse kaos er en ting. En anden er, at smart city systemer kan være sårbare over for trusler, som måske ikke påvirker samfundsordenen, men kan være alvorlige for enkeltpersoner. For eksempel hvis helbredsdata eller andre personlige oplysninger kommer i forkerte hænder.

Danmark er et af de lande, hvor borgerne har mest tillid til myndighederne. Herunder ligger, at borgeren har tillid til, myndighederne benytter data om borgeren til samfundsgavnlige formål og samtidig sikrer mod bevidst og ubevidst misbrug af følsomme personoplysninger. Denne tillid er det vigtigt at værne om. Samtidig er det lovpligtigt at beskytte persondata i henhold til persondataforordningen. Reglerne er stadig nye, og mange er forståeligt nok usikre på, hvordan de skal fortolkes i forbindelse med eksempelvis smart city projekter.

Reglerne i persondataforordningen bygger på en række principper.

// 1. Ansvarlighed (Respekt for borgerens data)
// 2. Formål (AI dataindsamling har et konkret formål)
// 3. Dataminimering (Indsaml kun det data, som er nødvendigt)
// 4. Retmæssighed, fairness og transparens (Man må kun indsamle data lovligt (hjemmel) og det skal være gennemsigtigt for borgeren, hvordan data bruges.)

// 5. Rigtighed (Data skal være korrekt)
// 6. Fortrolighed (Data skal være forsvarligt beskyttet)
// 7. Opbevaringsbegrænsning (Slet data når det ikke længere bliver brugt)

Sidst, men ikke mindst må man være opmærksom på, at et smart city system, der bygger på smalbåndskommunikation, sjældent står alene. På et eller andet tidspunkt bliver der typisk trukket data ud af systemet. Disse data behandles videre i kommunens øvrige IT-systemer – herunder menneskenes internet – og kan dermed være udsat for mange af de samme risici, som vi kender fra IT-sikkerhed generelt.

/ Smart city sikkerhed trin for trin /

Etableringen af et smart city system kan anskues som en række faser.
Det er vigtigt at tænke sikkerheden med hele vejen.

Trin 1: Få styr på rammerne

Arbejdet med at opbygge sikre smart city løsninger vil stort set altid være et samarbejde på tværs af fagcentre i en kommune i tæt parløb med en eller flere leverandører. Behovet for at arbejde med et smartcity system opstår typisk i et fagcenter som fx Teknik og Miljø eller Sundhed og Omsorg, og viden om sikkerhed ligger typisk i en IT-afdeling eller lignende.

Hvis du skal i gang med at arbejde med smart city projekter – og herunder sikkerhed – vil det være godt at starte med at få styr på rammerne for etableringen af smart city systemer, samt at orientere dig om, hvem i organisationen, der skal inddrages.

Start med stille dig selv eller din nærmeste leder følgende spørgsmål:

- ☐ Hvem kan sætte smart city projekter i gang? (Beslutningsproces)
- ☐ Hvem har ansvar for sikkerhed i løsningerne? Herunder ansvarsfordeling mellem fagcenter og IT-afdeling. Vær opmærksom på, at ISO 27000 serien af standarder kan anvendes som inspiration (Roller og ansvar)
- ☐ Hvem har viden og kompetencer om sikkerhed i organisationen – eksempelvis Databeskyttelsesrådgiver (DPO), lokale informationssikkerhedsmedarbejdere, IT-afdeling m.fl.? Hvilke fagpersoner skal inddrages med henblik på, at den rigtige sikkerhedsløsning i forhold til projektets formål bliver valgt?
- ☐ Hvilke procedurer skal følges både i pilotfasen, anskaffelsen, implementeringen og overleveringen til drift? (Anskaffelsesproces)
- ☐ Er der retningslinjer for integrationer og samspil med andre interne og eksterne systemer? (IT-arkitektur)
- ☐ Findes der lokale regler, sikkerhedsstandarder eller lignende? (Regler, standarder mv.)
- ☐ Er der retningslinjer for, hvordan man som kommune sikrer, at de løsninger, der sættes op, lever op til vedtagne sikkerhedsstandarder? (Kontroller eller andet)

// Sagt kort: Start dit projekt med at orientere dig i de lokale rammer for at køre et teknologiprojekt med fokus på sikkerhed. Afklar herunder hvilke videnspersoner i organisationen, du kan trække på.

Trin 2: Afklaring af projektets formål

Ny teknologi er spændende, men inden man begynder at forelske sig i bestemte tekniske løsninger, er det vigtigt at klarlægge, hvilken udfordring man ønsker at løse. Og ikke mindst, hvem man vil løse det for. Allerede her skal sikkerhed tænkes ind.

EU's persondataforordning indeholder et krav om "proportionalitet", der betyder, at et smart city system kun må opsamle de data, der er nødvendige for at understøtte et givent formål. Derfor er det vigtigt at arbejde præcist med projektets formål og have styr på hjemmel til opsamling af data.

Når man fx indsamler trafikdata via intelligent kamera, har man måske kun behov for at arbejde videre med "tællingen" – dvs. fx antal cykler, biler og fodgængere i et defineret tidsinterval. I så fald kan man undlade at gemme eller sende persondata, selvom tællingen bliver foretaget på baggrund af en billedstrøm, der i råt format indeholder persondata. I dette tilfælde understøtter persondata ikke formålet, og dermed kan projektet scopes ned til kun at omfatte data, der ikke er personhenførbare – nemlig tællinger per tidsinterval.

For at blive skarp på formålet kan du stille dig selv følgende spørgsmål:

- ☐ Hvad er formålet med smart city løsningen?
- ☐ Hvor lang tid skal løsningen køre?
- ☐ Hvilke data er der behov for, for at understøtte formålet?
- ☐ Hvilke kilder til data skal indgå?
- ☐ Har kommunen hjemmel til opsamling af den data, der er nødvendig til at understøtte formålet?

Hvis der er behov for at arbejde med persondata, vil data i så fald kunne enten anonymiseres eller aggregeres, så data ikke længere er personhenførbare – og stadig understøtte formålet? Hvis det er nødvendigt at arbejde med persondata – og disse ikke kan anonymiseres eller aggregeres – vil det med stor sandsynlighed være nødvendigt at foretage en risikovurdering og måske desuden en konsekvensanalyse. Det anbefales allerede i denne indledende fase at have en tæt dialog med organisationens Databeskyttelsesrådgiver (DPO) eller andre i organisationen med særligt ansvar for implementering af EU's persondataforordning.

// Sagt kort: Gør dig klart, inden du begynder at snakke med leverandører, hvilket formål dit system skal opfylde og, hvad det betyder for sikkerhed i løsningen.

Trin 3: Afdækning af it-sikkerhed og databeskyttelse

Beskrivelsen af den udfordring, som systemet skal løse, kan oversættes til behov for hardware, software og kommunikationsteknologi. Valgene har stor betydning for sikkerheden. Derfor er det nødvendigt at foretage en konkret sikkerhedsanalyse, der viser, hvordan risikoen for angreb på de enkelte dele kan minimeres.

Sørg for at følgende er på plads, inden projektet sættes i gang:

// **Foretag analyse af it-sikkerheden:** Involvér IT-afdelingen i denne del. Hver komponent og hvert del-system har et antal angrebsflader, som skal kortlægges med henblik på forebyggelse. Se også "Guide til sikkerhedsanalyse" sidst i dette kapitel.
// **Udarbejd risikovurderinger i forhold til databeskyttelsen:** Involvér kommunens Databeskyttelsesrådgiver (DPO) – og få hjælp til udarbejdelse af nødvendige risikovurderinger, herunder eventuelt forretningsmæssig risikovurdering, og eventuelt en konsekvensanalyse.
// **Få styr på lovgivning:** Undersøg med husets jurister, databeskyttelsesrådgiver eller lign. om systemet generelt lever op til gældende lovgivning – herunder fx EU's persondataforordning, serviceloven, forvaltningsloven, frekvensloven (der ved brug af LoRaWAN skal beskytte andre mod at blive generet af kommunens kommunikation), eller anden relevant lovgivning.

Hvis løsningen omfatter persondata, så undersøg:

- ☐ Adgang: hvem, skal have adgang til data, og hvordan administreres brugeradgang?
- ☐ Samkørsel: mulige effekter, hvis data samkøres med andre datakilder i visualiseringen. Der findes eksempler på, at anonymiserede data bliver personhenførbare igen, når data samkøres med flere informationer.
- ☐ Opbevaring og sletning: hvor længe opbevares data og hvornår slettes de?
- ☐ Oplysningspligten: hvem skal informeres omkring dataindsamlingen?
- ☐ Privacy by design/default: persondataforordningen stiller krav om at systemer, der behandler persondata, som skal designes og konfigureres så det understøtter sikkerhed i systemet.

// Sagt kort: Foretag sikkerhedsanalyse (kortlæg angrebsflader og forebyggende foranstaltninger), foretag risikovurdering, få styr på relevant lovgivning og vær opmærksom på særlige forhold omkring brug af persondata. Se også vores guide til sikkerhedsanalyse sidst i dette kapitel.

Trin 4: Kravsspecifikation.

En god kravs-beskrivelse er fundamentet for, at de interesserede leverandører kan formulere deres løsninger. Sørg for at din kravsspecifikation til en sikkerhedsløsning indeholder de syv punkter, som nævnes her neden for. Bed leverandøren beskrive præcist, hvordan de syv punkter tænkes opfyldt. Det kan godt være, at du ikke selv kan bedømme kvaliteten af svarene, men beskrivelsen vil om ikke andet gøre det muligt for dig at indhente en "second opinion".

De syv punkter er:

- ☐ **Krav #1: Hemmeligholdelse**
  Persondata og andre data, som kræver hemmeligholdelse, skal kun kunne tilgås af autoriserede brugere og være beskyttet af kryptering og/eller anonymisering.
- ☐ **Krav #2: Beskyttelse mod uønsket ændring**
  Data skal være sikret mod, at uvedkommende kan ændre i dem. Integriteten af data kan sikres med tjek af autenticitet via signatur, kryptering, brugerautorisering og lignende.
- ☐ **Krav #3: Tydelig kilde til data**
  Det skal være klart, hvor data kommer fra, herunder hvem der har oprettet data.
- ☐ **Krav #4: Retten til at teste**
  Nogle leverandører forbeholder sig, at man ikke må forsøge at hacke den leverede løsning. Det er vigtigt, at du sikrer dig ret til at teste, om systemet faktisk har den sikkerhed, som er aftalt.
- ☐ **Krav #5: Overholdelse af standarder**
  For mange typer af udstyr og systemer til smart city anvendelser findes der etablerede standarder. Det gælder fx de såkaldte Top 20 telco standards. Eksempler er ISO 27000 serien (information security management), ISO 31000 serien (risk management), ISACA COBIT 5, NIST SP 800 – 61 (computer security incident handling guide) samt PCI DSS (payment card industry data security standard).
- ☐ **Krav #6: Sletning af data og kassation af udstyr**
  Det er god digital hygiejne at sørge for, at data, som ikke længere er nødvendige, bliver slettet. Tilsvarende, at kasseret udstyr er renset for data.
- ☐ **Krav #7: Styr på opdateringer**
  Løbende opdateringer og vedligeholdelse af sikkerhedsløsningerne er vigtige. Skriv dette ind i kravsspecifikationen.

// Sagt kort: De syv nævnte krav bør indgå i din kravsspecifikation. Bed leverandøren specificere, hvordan de syv punkter tænkes opfyldt.

Trin 5: Udbud og anskaffelse.

Udviklingen af smart city systemer er endnu på et stade, hvor der er behov for innovative løsninger. Derfor er det ikke muligt at lægge alle forhold af betydning for sikkerhed og privacy fast som krav i udbudsmaterialet. Det er typisk hensigtsmæssigt, at de endelige løsninger findes gennem en dialog mellem kommunen og leverandøren.

Vigtige forhold, der overvejes i udarbejdelsen af en kontrakt, såfremt de ikke er en del af en kravspecifikation, der ligger til grund for kontrakten:

- ☐ Løsningen skal overholde love og regler.
- ☐ Kommunen har rettigheder til at teste løsningen for at verificere forhold omkring it-sikkerhed og privacy.
- ☐ Kommunen skal have mulighed for at tilgå rå-data, for eksempel i forbindelse med sikkerhedstest af systemet.
- ☐ Ejerskabet til data ligger hos kommunen.
- ☐ Aftalen bør også beskrive hvordan, og i hvilket format, kommunen har adgang til data i tilfælde af opsigelse af kontrakten.

I praksis kan det forekomme, at en leverandør behandler data på vegne af kommunen. I denne situation er det vigtigt, at der etableres en databehandleraftale med leverandøren.

// Sagt kort: Gå i dialog med leverandøren. Stå fast på, at du vil have ret til at teste sikkerheden og, at kommunen ejer data og at vil have mulighed for at tilgå rå-data.

Trin 6: Drift og governance.

Mange smart city projekter begynder som pilotprojekter. Det er ikke altid de medarbejdere, der har deltaget i pilotprojektet, som kommer til at stå for tingene senere, når man går over til fuld drift. Det er vigtigt, at der sker en grundig overlevering. Få gjort klart så tidligt som muligt, hvem der har ansvar for hvad i drift-situationen – og sørg for at involvere disse personer så tidligt som muligt i projektforløbet. Blandt andet er det vigtigt, at man har taget stilling til, hvor ofte systemerne skal opdateres – eksempelvis med sikkerhedsopdateringer (såkaldte patches). Skriv ned, hvem der har ansvaret for, at det sker. Desuden hvordan fejlrapporteringer håndteres.

Endelig er det klogt at have en såkaldt exit-strategi. Skulle det eksempelvis ske, at systemet ikke lever op til forventningerne, hvordan kan man så komme ud af samarbejdet – uden at der opstår forringet service for borgerne eller forstyrrelse af andre systemer? Herunder bør det sikres, at der tages hånd om de data, der er genereret i projektet: skal de slettes eller har det et formål at lagre dem?

Følgende er en huskeliste, du kan bruge, når du sætter navne på de ansvarlige for de forskellige elementer inden for drift og governance.

- ☐ Hvem har ansvar for, at patches fra leverandører bliver implementeret?
- ☐ Hvem har ansvar for håndtering af fejlrapporteringer?
- ☐ Hvem har ansvar for sletning af data, som ikke længere er aktuelle?
- ☐ Hvem har ansvar for etablering og vedligeholdelse af exit-strategi?

// Sagt kort: Sørg for tidligt at få afklaret opgaver og ansvarsforhold i drift-situationen. Hav en exit-strategi.

Hvad er personoplysninger?

En personoplysning er enhver form for information, der kan henføres til en bestemt person, også selv om personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger. Personoplysninger kan for eksempel være personnumre, registreringsnumre, et billede, et fingeraftryk, en stemmeoptagelse, lægejournaler eller biologisk materiale, når det i praksis er muligt at identificere en person ud fra oplysningerne eller i kombination med andre oplysninger.

Selv om oplysninger som et navn eller en adresse er erstattet af en kode (...) er det stadig en personoplysning, hvis koden kan føres tilbage til den oprindelige personoplysning. Det er tilfældet, så længe der er nogen, der kan gøre oplysningerne læsbare og identificere de personer, det drejer sig om. Dette kaldes ofte pseudonymiserede oplysninger, og sådanne oplysninger er fortsat omfattet af databeskyttelsesreglerne.

På samme måde er summarisk behandling af oplysninger om flere individer, som er blevet samlet og kombineret uden fokus på det enkelte individ kun anonyme, hvis der ikke er nogen, der kan genkende personerne ud fra oplysningerne eller ved kombination med andre oplysninger. Dette kaldes ofte aggregerede oplysninger, og det vil afhænge af en konkret vurdering, om sådanne oplysninger er omfattet af databeskyttelsesreglerne.

Oplysninger, der er gjort anonyme, sådan at ingen fysiske personer kan identificeres ud fra oplysningerne eller i kombination med andre oplysninger, er ikke længere beskyttet af databeskyttelsesreglerne.

Kilde: Datatilsynet.
http://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger

/ Guide til smart city sikkerhedsanalyse /

Formålet med denne guide er at bygge bro mellem smart city fagpersoner og personer med sikkerhedsviden, eksempelvis i en kommunes IT-afdeling.

Hvad er en sikkerhedsanalyse?

En sikkerhedsanalyse er en vurdering af IT-tekniske trusler og sårbarheder. Dette kaldes også en teknisk risikoanalyse.

Forud for den tekniske sikkerhedsanalyse foretages en risikovurdering. Hvilke konsekvenser vil det have, hvis der sker et nedbrud, indtrængen eller lignende? Kan der fx ske læk af persondata, eller kan vigtige samfundsfunktioner blive lagt ned?

Næste trin er at kortlægge systemet og teknologien.

Et smart city system består oftest af:

// Sensorer/kameraer, der opsamler data
// Netværk, der overfører data (Fx LoRaWAN, NB-IoT, SigFox, GSM eller WiFi)
// En server hvortil data overføres og
// En applikation (software) som behandler data.
// Automatisering eller visualisering – data benyttes enten til brug for et andet it-system (fx automatisering af et lyskryds) eller de benyttes i et visualiseringsværktøj (til beslutningsstøtte eller lign.).

Hver komponent og grænsefladerne mellem dem kan betragtes som en angrebsflade. Altså en indgangsvinkel til at forsøge at kompromittere systemet. Som minimum bør man identificere alle systemets komponenter og deres grænseflader (de såkaldte API'er; Application Programming Interfaces) mod andre komponenter. For de grænseflader, der er tilgængelige fra internettet, bør man sikre, at kravsspecifikationens krav til hemmeligholdelse, beskyttelse mod uønskede ændringer samt tydelig angivelse af kilder til data overholdes.

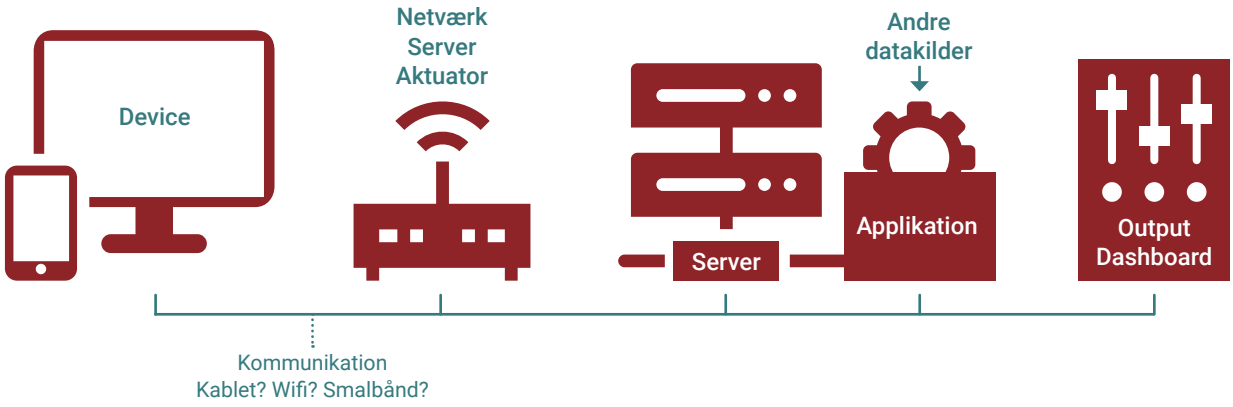
Det er vigtigt at kortlægge systemet i brug, når man vil identificere de mulige angrebsflader og de metoder, som en angriber vil kunne benytte sig af. På trods af, at den overordnede struktur typisk er den samme, er der nemlig altid strukturer, som er specifikke for det enkelte system. I LoRaWAN vil man typisk kigge på end-device, gateway (aktuator), netværksserver, applikationsserver samt kommunikationen, som i LoRaWAN sker via radiofrekvenser. Eventuelt kan man eksperimentelt afprøve – ved hjælp af en venligtsindet hacker – om indtrængen er mulig.

Fjerde trin er at afklare konkrete sikkerhedsløsninger og forebyggende foranstaltninger.

Endelig lægger man sig fast på sine sikkerhedsløsninger og forebyggende foranstaltninger. Her inddrages risikovurderingen, så man sørger for at have størst fokus på de områder, hvor konsekvenserne af brud på sikkerheden vil være mest alvorlige.

Hvad er det særlige ved sikkerhedsanalyse i smart city sammenhæng?

Fundamentalt minder smart city løsninger meget om andre IT-løsninger. En stor del af sikkerhedsanalysen bør derfor fokusere på devices, infrastruktur, datalagring, tjenester og kommunikationen mellem delene – helt som ved andre IT-systemer. Det særlige i smart city sammenhæng består i, at en stor del af kommunikationen foregår i det offentlige rum. Dette betyder, at der er en større



fysisk angrebsflade tilgængelig. Dermed er der ekstra grund til at være opmærksom på spørgsmålene omkring databehandling, herunder kryptering, samt tele-planlægning. Det er også ekstra vigtigt at sørge for, at applikationer – særligt web-applikationer – har autoriseret adgang. Desuden bør kommunikationen være beskyttet af kryptering og autentificering, så kun afsender og modtager kan læse informationen, der sendes mellem dem.

Hvad analyserer du – og hvordan?

// **Punkt 1:** Foretag en vurdering af trusselsbilledet og sårbarheder. Beskriv kompleksiteten i løsning/set-up, herunder leverandørens modenhed, insider-trusler mv. Som inspiration kan du finde de ti største trusler og sårbarheder inden for Internet-of-things i OWASPs anerkendte liste: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.

// **Punkt 2:** Overvej beskyttelsen af dine data, herunder kommunikationen. Mulige løsninger: Kryptering og/eller sikker kommunikation via VPN (Virtual Private Network) eller lignende. Desuden bør man inkludere løbenumre eller tidsstempler for at sikre friskhed (freshness) i datapakker, hvilket beskytter mod, at en angriber opnår fordele ved at gensende tidligere opsnappet kommunikation.

// **Punkt 3:** Sørg at have effektiv backup for dine data samt recovery procedurer, så evt. tabte data kan retableres.

// **Punkt 4:** Sørg for at sikre backend-servere, fx med firewall, der definerer regler for gyldig kommunikation på serverne. Man kan bl.a. bruge DNS-filtrering og multiservermiljø.

// **Punkt 5:** Husk at inddrage sikkerheden omkring visualiserings-værktøjer og modtagersystemet i øvrigt. Bl.a. er det vigtigt, at applikationerne er i stand til at detektere unormal aktivitet.

// **Punkt 6:** Password-sikkerhed. Der bør bl.a. være krav til passwords, som følger gældende anbefalinger mht. længden af passwords mv. Der findes gode råd i vejledning fra Center for CyberSikkerhed (https://fe-ddis.dk/cfcs/publikationer/Documents/Vejledning-Passwordsikkerhed.pdf).

// **Punkt 7:** Opstil regler for brugerrettigheder, herunder hvilke "roller" i organisationen, der skal have adgang til forskellige niveauer af systemet. Inddrag Identity & Access Management, rettigheder som privilegeret bruger, samt sikkerhedsklassificering.

// **Punkt 8:** Dataskik, sikkerhedsdokumentation og persondata (persondataforordningen). Procedurer for sletning af overflødige data. Endvidere anonymisering, kryptering eller sløring (hashing) af persondata. Se også boksen "Hvad er personoplysninger?".

// **Punkt 9:** Fysisk sikkerhed. Hvem har fysisk adgang (analog eller virtuel nøgle) til installationerne? Er aflåste bokse forsynet med såkaldt tamper protection, som sørger for, at de lukker ned, hvis nogen trænger ind uden at bruge en gyldig nøgle/adgangskode?

// **Punkt 10:** Netværkssikkerhed.
Mulige løsninger: Adgangskontrol, der blokerer uautoriserede brugere/devices. Anti-malware, der bekæmper virus, worms, trojans etc. Desuden application security, der kan lukke usikre apps ned. Overvågning og analyse af afvigende opførsel af netværket. Sikring af e-mails mod phishing ved hjælp af filtre og modeller for tekstanalyse. Etablering af en baseline for datapakker – dette kan benyttes som udgangspunkt for beskyttelse mod indtrængen (IDS – Intrusion Detection and Prevention), dvs. systemer, som skanner netværket og blokerer angreb ved at sammenligne aktiviteten på netværket med kendte angreb. Netværks-segmentering, der deler netværket op i klasser med henblik på at begrænse omfanget tab. VPN (Virtual Private Network), der verificerer kommunikation mellem device og netværk i en krypteret kanal.

// **Punkt 11:** Sikkerhed for bærbare enheder som smartphones og tablets. For det første skal man sikre sig, at mobile enheder kun forbindes gennem sikre netværk eller benytter sikre protokoller (fx TLS, HTTPS, SSH eller SFTP), når de forbinder gennem usikre netværk. Hernæst skal man sikre, at data lagret på de mobile enheder ikke mistes, hvis enheden bliver tabt eller stjålet. Hvis det er muligt, bør data krypteres, når de lagres på mobile enheder. Alternativt kan data lagres centralt – i skyen – hvilket kræver effektive producerer til at blokere adgang i tilfælde af, at enheden tabes eller stjæles.

// **Punkt 12:** Beredskabsplaner. Procedurer for, hvad man gør i tilfælde af, at systemet bliver kompromitteret. Alt afhængigt af, hvilken type smart city system, der er tale om, vil det være meget forskelligt, hvordan beredskabsplanen ser ud. Derfor er det ikke muligt at give en konkret anbefaling. Det er nødvendigt at definere beredskabsplanen for hvert system.

// **Punkt 13:** Overholdelse af standarder. Der findes en række internationale standarder, der kan benyttes som reference. Eksempler er ISO 27000 serien (information security management) samt ISO 31000 serien (risk management). Gode alternativer eller supplerende værktøjer er OWASP samt Common Weakness Scoring System (CWSS). Læs mere om disse værktøjer i håndbogens tekniske sektion.

// **Punkt 14:** Audit-muligheder. Med den enkelte leverandør aftales i forbindelse med forhandlingerne om kontrakt, at man som kunde kan teste systemet. Herunder er det vigtigt at sikre sig lov til såkaldt penetration tests og helst også reverse engineering med henblik på at efterprøve sikkerheden af løsningerne.

// **Punkt 15:** Leverandørens medansvar og investeringer i sikkerhed. Som udgangspunkt er der ingen regler, der lægger leverandørens ansvar for udvikling af sikkerheden i smart city løsninger fast. Imidlertid er dette noget, man har mulighed for at inddrage som en del af kontraktforhandlingen med leverandøren.

// **Punkt 16:** Leverandørens engagement/forpligtelse med hensyn til sikkerhedsopdateringer. Hvis leverandøren ikke lover eller vurderes i stand til at levere sikkerhedsopdateringer i hele systemets forventede levetid, bør man overveje at vælge en anden leverandør.

Nyttige tips:

Overvej beskyttelsen mod jamming, replay attacks (gensendelse af opsnappet gammel kommunikation) samt relay attacs (hvor angriber sender data videre på en måde, så enheder tror, at de er i nærheden af hinanden, hvilket for eksempel er et problem for systemer til adgangskontrol med trådløs læsning af adgangskort). Disse typer angreb forekommer hyppigt.

Placer så vidt muligt hardware, hvor der ikke er adgang for uvedkommende.

Kør regelmæssige sundhedstjek af systemets data. Etabler herunder en baseline for datapakker. På den måde kan du overvåge udsving og blive alarmeret, hvis der sker markante begivenheder.

/ Hent inspiration /

Smarter Denmark
Projektmagere inden for Smart City løsninger kan ofte slippe for at opfinde de dybe tallerkener selv. Der er allerede en lang række projekter derude, lige fra selvkørende busser over intelligent belysning på skoler til selvoptimerende rensningsanlæg. Et godt sted at finde inspiration er case-samlingen på hjemmesiden for Smarter Denmark, som er et fællesoffentligt Smart City partnerskab bestående af Danske Regioner, Digitaliseringsstyrelsen, Erhvervsstyrelsen, Kommunernes Landsforening (KL) og Styrelsen for Dataforsyning og Effektivisering.

https://smarterdenmark.kl.dk

Sikker Digital
På sikkerdigital.dk kan borgere, virksomheder og myndigheder finde viden, vejledning og konkrete værktøjer til en sikker digital hverdag. Bag sikkerdigital.dk står Digitaliseringsstyrelsen og Erhvervsstyrelsen, samt en række samarbejdspartnere. Her er blandt andet skabeloner og værktøjer til it-beredskabsplaner, it-sikkerhedspolitikker, risikovurderinger og teknologivurderinger.

https://sikkerdigital.dk/

// Case:

Bedre styr på parkeringssynderne i Frederiksberg Kommune

Frederiksberg Kommune samarbejder med teknologi-leverandøren Schweers om en tjeneste, der gør det lettere at holde styr på registreringen af parkeringsafgifter. Sparet tid er sparede omkostninger. Løsningen forudsætter imidlertid, at reglerne om beskyttelse af personoplysninger (persondataforordningen) er overholdt.

Den grundlæggende identifikation i systemet bygger på, at parkeringsvagten, som udskriver parkeringsafgifter, skanner bilens nummerplade med en håndskanner med indbygget kamera og samtidig logger dels tidspunktet, dels den nøjagtige position med GPS. Næste skridt er en sammenligning med backoffice-systemet Politess og økonomisystemet Prisme, som bruges til at administrere afgifterne. Politess driftes af Schweers og registrerer alene nummerplade og informationerne om afgiften. Via SKATs motorregister identificeres ejeren af bilen. Herefter kan kommunen opkræve afgiften hos ejeren af bilen ved hjælp af økonomisystemet Prisme.

Systemerne er indrettet, så kun få autoriserede medarbejdere i kommunen har adgang til samtlige systemer. Derved er risikoen for læk af data minimeret. Den samlede løsning er opbygget, så personoplysninger beskyttes bedst muligt. Herunder, at det ikke er muligt at følge personers færden i byrummet.

Løsninger:

Ud fra et privacy-by-design princip er det vigtigt, at følsomme personoplysninger bliver anonymiseret straks ved indsamlingen af data. Det kan ske på flere måder. For det første registreres modtageren af afgiften – bilens ejer – ikke med sit CPR-nummer. Yderligere beskyttelse af personoplysningerne i projektet var temaet for et såkaldt Hackaton, som Smart City Cybersecurity Lab og Frederiksberg Kommune holdt i samarbejde med DTU Compute's HackerLab og DTU's laboratorium for studenterinnovation, DTU Skylab. De studerende undersøgte sårbarhederne og anviste samtidig løsninger. En af anbefalingerne er, at nummerpladen anonymiseres ved hjælp af et matematisk værktøj, der genererer en ny kode. Det samme kan ske for oplysningerne om positionen og tidspunktet. Frederiksberg Kommune overvejer at indføre disse værktøjer, som især vil være relevante, hvis kommunen senere ønsker at anvende data til andre formål, eksempelvis planlægning af trafikken, placering af parkeringspladser eller lignende.

Det samlede sæt af informationer har kun værdi, så længe der er ubetalte afgifter. Imidlertid siger forvaltningsloven, at kommunen skal opbevare data i tre år. Herefter er der ingen grund til at opbevare informationerne længere. Med andre ord er det muligt at lægge ind i systemet, at informationerne slettes, når de tre år er gået. Dermed mindsker man risikoen for læk af personoplysninger yderligere samtidig med, at man sparer server-kapacitet og strømforbrug.

Interview;
Hasse Hauch,
GIS og digitaliseringschef,
Frederiksberg Kommune.

Fra en spole i vejen til kunstig intelligens

Der er rige muligheder for at hente merværdi fra smart city systemer. Forudsætningen er at finde det rigtige niveau af sikkerhed.

"I mange år har det virket fint at lægge en slange over vejen og på den måde få data for trafikken. Men nu er det på tide at tage det næste skridt. Når vi sætter et kamera op og kombinerer optagelserne med billedanalyse ved hjælp af kunstig intelligens, tæller vi ikke kun bilerne. Vi kan også se, hvilke typer af biler, der er tale om, og vi kan se, hvordan fodgængere og cyklister bevæger sig. Vi kan også få andre informationer. Hvor mange cyklister kører med cykellygter, hvor mange bruger cykelhjelm? Det er blot et af mange eksempler på, hvordan vi kan hente merværdi."

Som GIS og digitaliseringschef har Hasse Hauch det overordnede ansvar for arbejdet med smart city systemer i Frederiksberg Kommune, som gennem flere år har arbejdet strategisk med området.

"Der er i nogen grad frygt for læk af data og andre sikkerhedsrisici, når der arbejdes med smart city projekter. Der er nogle områder, hvor der er betydelig risiko, men der er også andre, hvor der vitterligt er meget lille risiko. Det handler om at få afdækket, hvornår der er risiko, og hvornår der ikke er," siger Hasse Hauch.

Se dit kamera som en billedsensor

Brugen af kameraer til at samle data ind om trafikken er et eksempel:

"Vi har jo ingen ønsker om at identificere de enkelte individer i trafikken. Derfor kan vi sætte systemet op, så data anonymiseres straks ved indsamlingen. Man kan se sådan på det, at enheden i virkeligheden er en billedsensor snarere end et kamera. Gør man dette rigtigt, er der ingen risiko, selv hvis der skulle ske læk af data – da det jo slet ikke er persondata, som bliver indsamlet."

En anden udfordring er at sørge for, at de løsninger, som udvikles inden for anonymisering og cybersikkerhed, kan benyttes ud over det konkrete projekt.

"Mange projekter anvender 1. generation af en teknologi. Vores samarbejdspartnere er ofte forskere ved universiteterne og mindre, innovative virksomheder. Her er det vigtigt at tænke ind, at løsningerne skal kunne skaleres op, når man går fra pilotprojekt til fuld anvendelse og almindelig, daglig drift. Problemet er nogle gange, at de medarbejdere, der har deltaget i pilotprojektet, er nogle andre end dem, som senere skal stå for at sende projektet i fuld skala i udbud."

Tag brodden af frygten

Samtidig understreger Hasse Hauch, at han ikke forsøger at bagatellisere sikkerhedsudfordringerne:

"Det er jo reelt nok, at man har en bekymring. Der er vitterligt områder, hvor det er supersvært at finde den rigtige balance. I den enkelte situation må man starte med at spørge sig selv: Vil der blive indsamlet persondata i det system, jeg overvejer? Og hvis svaret er ja, er det så muligt at anonymisere disse data? Der kan måske være projekter, som man bliver nødt til at holde sig fra, men det vigtige er, at man ikke bliver handlingslammet. Opgaven for os, der arbejder på feltet, må være at tage noget af brodden af frygten. Og synliggøre, at der er forskellige niveauer af risiko, og at det niveau af risiko, som vi accepterer, skal stå mål med effekten af projektet."

// Case:

Fleksibel regulering af trafikken i Vallensbæk

Traditionelt er trafiklys programmeret til at skifte mellem grønt, gult og rødt med bestemte intervaller. Først hvis man konstaterer, at trafikken flyder dårligt, kan man programmere om og se, om det nu går bedre. Et nyt system, som et regionalt støttet projekt med bl.a. operatøren Gate 21 og leverandøren Technolution forbereder i samarbejde med Vallensbæk Kommune, skal selv tilpasse styringen automatisk ved at registrere trafikudviklingen. Vel at mærke går man ikke over til et nyt, fast skema. Systemet tilpasser sig så ofte, der er behov for det.

Systemet er baseret på såkaldt Floating Car Data, der genereres ud fra GPS-data. Vel at mærke sker der ikke nogen fotografering af bilerne eller lignende, som kunne bruges til at registrere køretøjer eller personer. Dermed er der ingen følsomme personoplysninger i projektet og heller ingen risiko for at overtræde reglerne i persondataforordningen. Alligevel er det naturligvis vigtigt at afdække sikkerhedsforholdene. Dette har Vallensbæk Kommune, Gate 21 og Technolution gjort i et separat forprojekt.

Den gode nyhed i afdækningen af sikkerheden er, at trafiklys ikke er blandt de mest oplagte mål for hackerangreb fra organiserede kriminelle. Der er ingen mulighed for at skaffe sig adgang til personoplysninger eller til umiddelbar berigelse. Man kunne ganske vist forestille sig, at kriminelle kunne udnytte kontrol med trafiklysene i forbindelse med flugt efter et røveri, men risikoen må vurderes som beskeden – samtidig med at skadevirkningerne for samfundet ville være begrænsede. Det vurderes også, at risikoen for, at trafiklys bliver mål for terrorangreb, er lille. Ganske vist er der betydelig risiko for skade på personer, hvis et trafiklys eksempelvis viser grønt fra begge retninger, men formentligt vil terrorister vurdere, at effekten er for beskeden i forhold til den indsats, som de skulle lægge i at hacke sig ind i styringen.

Derfor samler opmærksomheden sig om hackerangreb med mere diffuse formål som at forstyrre den offentlige orden. En måde at angribe systemet kunne være at gå via det kontrolpanel, som tænkes anbragt i en boks ved lyskrydset. Typisk konfigureres trafiklyset via en forbindelse, som enten kan være en fjernbetjening eller en port i kontrolpanelet. I begge tilfælde kan en angriber, som er fysisk til stede i lyskrydset, forsøge at opsnappe stumper af kommunikationen mellem trafiktælleren og kontrolpanelet. Disse stumper af kommunikation kan udnyttes til at fabrikere information, som systemet vil opfatte som data, der er genereret af systemet selv.

Endelig er det muligt at angribe trafiklyset via kontrolsystemets front mod omverdenen. En angriber vil typisk lede efter sårbarheder i kommunikationen og i applikations-serveren, netværks-serveren og andre former for hardware. Sårbarhederne kan udnyttes til at sende falske beskeder ind i systemet. Det kan også være muligt at gen-sende data, som systemet selv har skabt. På den måde kan man for eksempel narre systemet til at tro, at der kører langt flere biler gennem krydset, end der faktisk gør. Endelig kan sårbarhederne udnyttes til at jamme systemet – altså fylde det med digital støj, så det til sidst må lukke ned.

Fælles for disse sårbarheder er, at de er generelle for smart city systemer. Fordi systemerne stort set altid bygger på et større antal enheder, der er anbragt i det offentlige rum og langt fra et centralt kontrolcenter, er den fysiske angrebsflade, som en indtrænger har mulighed for at benytte sig af, meget stor. Til gengæld er der også gode muligheder for at forebygge, at indtrængen i en enkelt enhed fører til større skadevirkninger.

Løsninger:

Der findes en række tekniske værktøjer, som kan bruges til at beskytte et trafiklys. Et eksempel er, at man kan forsyne de fleste typer hardware i systemet med switches, der lukker en enhed, som er kompromitteret, ned. Tilsvarende bør den boks, som rummer trafiklysets kontrolpanel, være beskyttet med en mekanisme, som lukker panelet, lukker ned, hvis boksen åbnes uden brug af systemnøglen. Desuden bør trafiklysene være isoleret i forhold til hinanden. Med andre ord skal det ikke være muligt at tilgå andre trafiklys digitalt for en indtrængende, som er lykkedes med at nå ind i styringen af et enkelt trafiklys.

De forskellige løsninger beskrives nærmere i håndbogens tekniske sektion. Denne type løsninger er relevante i en lang række smart city systemer.

Den Regionale Datahub

Smart City Cybersecurity Labs sikkerhedsvurdering af de smarte trafiklys i Vallensbæk indgår i samarbejdet "Den Regionale Datahub" om sikker deling af data mellem kommuner. Dette projekt er igangsat og støttet af Region Hovedstaden og ledes af smart city samarbejdet i Gate 21. Det er muligt at læse mere om det overordnede formål med Gate 21 projektet samt sikkerhedsspørgsmålene her: https://denregionaledatahub.dk/

Sikker og Anvendt Data

Et andet projekt, der opbygger samarbejde og viden om sikkerhed i smart city, er projektet Sikker & Anvendt Data, der vil styrke anvendelsen af IoT-løsninger på tværs af kommuner for at skabe bedre mobilitet, klima og miljø. Her står DTU i regi af Smart City Cyberseurity Lab for arbejdspakken med sikkerhed og udvikling af adgangsmodeller for anvendelse af data. Projektet opbygger et datadrevet innovationsmiljø - "en sandkasse" - på tværs af kommuner, hvor de sammen kan teste og udvikle konkrete løsninger, hvor de bruger IoT- og anden data, og samarbejde om den underliggende tekniske infrastruktur. Projektet ledes af Gate21, Frederiksberg, Høje Taastrup og DTU med Region H, Ballerup, Vallensbæk og 13 andre kommuner som deltagere. Erfaringerne opsamles i en åbent tilgængelig wiki: http://iotwiki.dk/

Interview;
Jette Sørensen,
organisationskonsulent, Vallensbæk Kommune.

Udseendet tæller

Et praktisk tip: sørg for, at udstyr, som sættes op i byrummet, ikke skiller sig for meget ud fra omgivelserne.

"Sensorer, kameraer og andet udstyr, som du sætter op i byrummet, bør være sikret mod hærværk og falde naturligt ind. Det stiller krav til udseendet af udstyret. Det naturlige look, tænker jeg, kan bestå i alt fra det diskrete look til graffiti på udstyret. Det vigtige er, at det falder i med tapetet. Og så husk, at det ikke kun er mennesker, der begår hærværk. Overvej også, om edderkopper og andre dyr kunne have særlige motiver."

I forbindelse med smart city projekter vil Jette Sørensen ofte have rollen som projektleder.

"Jeg sidder i digitaliseringsteamet og er tæt på vores it-afdeling, men ofte er indkøberne ved smart city projekter fra andre fagområder. Her ser vi tit, at de har fokus på selve løsningen og implementeringen, mens spørgsmål som sikkerhed, drift og vedligehold naturligt fylder mindre, end det gør for it-folk."

Tænk drift ind i udbuddet

Et eksempel er senere opdateringer af systemer og sikkerhedssoftware – i fagsproget kaldet patches (plastre).

"Trusler og løsninger inden for cyber-sikkerhed er i stadig forandring. Derfor vil leverandørerne nødvendigvis komme med patches. Her er det vigtigt, at man har taget stilling til, hvor ofte systemerne skal opdateres, og til, hvem der har ansvaret for, at det sker," siger Jette Sørensen og tilføjer:

"Tilsvarende er det vigtigt at fastsætte tidsfrister for, hvornår data skal slettes. I mange situationer har man kun behov for at lagre data i et kortere tidsrum. Så bør man sikre, at de slettes. For det første er der ingen grund til, at overflødige data optager lagerplads, og for det andet slipper man for den risiko, der kunne ligge – hvis kommunen eksempelvis forærer IT-udstyr til et skoleprojekt, og det så viser sig, at der ligger data, som kan henføres til personer, på harddiskene."

Med andre ord bør der ligge en procedure for opdateringer og for sletning af data.

"Det er vigtigt at afklare, hvem der har ansvar for hvad i driftssituationen. Derfor vil jeg anbefale indkøbere at inddrage IT-afdelingen tidligt i projektet. Gerne allerede ved udarbejdelsen af kravsspecifikationen. Man må gøre sig klart, at de krav, som man stiller, også vil have en konsekvens for driften."

Forebyg data-forelskelse!

I det hele taget gælder det om at være skarp i de tidlige faser af processen:

"Du skal gøre dig klart, hvad du præcis ønsker at få ud af projektet. Hver gang du indbygger ekstra

elementer, vil der typisk også være ekstra strømforbrug og større slid på komponenter. Hvis du samtidig er for fokuseret på anskaffelsesprisen, risikerer du, at tingene har for kort levetid. Så kan de forbedringer i effektivitet, som er formålet med projektet, hurtigt blive spist op af omkostninger til at udskifte batterier og genanskaffe udslidte komponenter."

Ønsket om skarphed gælder ikke kun for det fysiske udstyr, men også for data, understreger hun:

"I disse Big Data tider er der en tendens til, at folk gerne vil kunne trække alle mulige former for data ud af deres smart city system. Men man skal huske på, at det koster arbejde og ressourcer, når man skal holde styr på store datamængder og strukturere dem på en måde, så de bliver brugbare. Dertil kommer eventuelt øgede sikkerhedsrisici. For eksempel ser man nogle gange, at data, som egentlig er anonymiserede, bliver de-anonymiserede. Man ønsker måske lige at indhente et nyt sæt af data og tænker ikke på, at når man sammenholder disse data med de anonymiserede data, bliver det pludselig muligt at identificere personer. Derfor er min anbefaling, at man starter med at klargøre sit forretningsbehov og designer sit system ud fra det. Pas på med at blive forelsket i data!"

Interview;
Bo Fristed,
chef for ITK, Aarhus Kommune.

Længe leve redundans

Kritiske smart city systemer bør være dublerede, både når det gælder indsamling og transmission af data.

"Selv med stor fokus på cybersikkerhed kan man ikke gardere sig fuldstændigt mod tekniske fejl og hacking. Så hvis jeg skal give én anbefaling til mine kolleger i kommunerne, må det være at indbygge redundans i de kritiske systemer."

Bo Fristed giver et eksempel, der er sørgeligt aktuelt. To dage før interviewet mistede en borger i Aarhus livet, da han faldt i havnebassinet.

Byrådet havde i forvejen bevilget penge til opsætning af varmefølsomme kameraer i havnen, men først på næste års budget. Tanken er, at overvågningen skal give automatisk besked direkte til beredskabet, hvis varme svarende til et menneske overskrider en virtuel grænse og dermed er på vej til at falde i vandet.

"Generelt er det meget vigtigt at være opmærksom på pålideligheden af systemerne, når vi i stigende grad overlader til teknikken at styre vores byer," siger Bo Fristed. "Konkret mener jeg, at kritiske systemer skal være baseret på to sæt separate sensormålinger og desuden på to separate kanaler for transmission af data. Det kan være overvågning af havnen, men også automatisk styring af trafiklys og lignende."

Lad maskinen klare det trivielle

"Når vi er i dialog med borgere og politikere, fylder diskussionen om privacy rigtig meget. Det forstår jeg godt, men jeg ville alligevel ønske, at vi kunne slippe for at starte helt forfra hver gang. GDPR-reglerne slår jo fast, hvad vi må og ikke må. Der er ingen kommuner, som har interesse i at indsamle data, som vi ikke må. Hvis vi nu kunne tage det som fællesnævner, kunne vi måske komme videre," lyder et hjertesuk fra Bo Fristed.

Her er det vigtigt at huske på de fordele, som digitaliseringen medfører:

"Vi kan lige så godt sætte maskiner til at udføre de opgaver, der er trivielle eller unødvendigt dyre at få mennesker til at udføre. Tag flyttemeddelelser som eksempel. Hver gang en dansker melder flytning, har kommunen pligt til at verificere, at indberetningen virker korrekt. Det sker fortsat manuelt i de fleste kommuner, men det er muligt at gennemgå indberetningerne automatisk med RPA (Robotic Process Automation, red.), så man kun behøver manuelt tjek af det lille antal indberetninger, der virker mærkelige. Den type løsninger kan spare rigtig mange ressourcer i kommunerne."

RPA er et af de emner, der behandles i fællesskabet Offentligt Samarbejde & Open Source (forkortet OS2). Bo Fristed er medlem af bestyrelsen for OS2, som er en medlemsforening for kommuner og andre offentlige myndigheder,

der sammen udvikler og deler løsninger åbent og tilgængeligt.

Populær kommunal krav-motor

OS2 har en række leverandørpartnere, som ønsker at understøtte open source og levere på åbne vilkår.

OS2 har blandt andet udviklet en såkaldt krav-motor, der understøtter udarbejdelsen af kravsspecifikationer.

"Krav-motoren kan understøtte den tekniske dialog mellem leverandøren og den offentlige myndighed i forbindelse med IT-indkøb og herunder naturligvis også løsninger inden for smart city cybersikkerhed. Vi vil gerne undgå, at alle landets 98 kommuner skal opfinde de samme løsninger hver for sig."

Foreløbigt har 68 kommuner og en region meldt sig ind i OS2.

"Vi kan se, at langt flere end medlemmerne bruger platformen. Det bekræfter mig i, at OS2 er et rigtig godt værktøj."

Fællesskabet OS2

Offentligt Samarbejde & Open Source (OS2) er en medlemsforening for kommuner og andre offentlige myndigheder, der sammen udvikler og deler løsninger åbent og tilgængeligt.

Blandt de produkter, som er udviklet i OS2, er:
OS2 kravmotor, som genererer de ikke-funktionelle krav til IT-anskaffelser. Dvs. at krav-motoren er et værktøj, der understøtter udarbejdelsen af kravsspecifikationen, hvor man kan vælge mellem forskellige standardfraser, som andre har brugt tidligere, eller som er skabt i fællesskab. OS2 kravmotor har foreløbigt 23 kommuner som deltagere.

OS2 kitos er et produkt, hvor man på tværs af kommuner kan se den samlede systemportefølje. Det giver bl.a. mulighed for at synkronisere – eller samarbejde om – udbud. OS2 kitos har 88 kommuner som deltagere.

Alle produkter i OS2 kan findes på: https://os2.eu/produkter

/ Overvejelser om sikkerhed i LoRaWAN /

På baggrund af eksperimenter konkluderer DTU Compute's Hackerlab, at det er muligt at forebygge en række almene sårbarheder i smart city LoRaWAN-systemer.

LoRaWAN (Long Range Wide Area Network) er et blandt flere systemer, der egner sig til smart city løsninger og tilsvarende kommunikation mellem maskiner (Internet-of-Things, dimsernes internet). Som nævnt tidligere i denne håndbog har mange danske kommuner valgt at basere kommunikationen i deres smart city systemer på LoRaWAN. Det har især to årsager. For det første er dele af LoRaWAN open source, hvilket giver gode muligheder for aktivt at teste og forbedre sikkerheden i løsningerne. For det andet giver LoRaWAN "meget smart city for pengene" – blandt andet fordi kommunen slipper for at betale abonnementer for de enkelte apparater i systemet.

Imidlertid er der sårbarheder forbundet med LoRaWAN, lige som der er sårbarheder i ethvert andet system. Hver eneste gang vi kobler systemer op til internettet eller til andre digitale platforme, vil der åbnes for usikkerhed. Tanken med denne håndbog er ikke at opnå nul-risiko. For det er en umulighed. I stedet drejer det sig om dels at beskytte sine systemer, dels at have strategier for, hvordan der skal reageres på angreb, og hvordan driftstilstanden skal genoprettes, hvis en indtrængende lykkes med sit forehavende.

Vi gennemgår her de forskellige problematikker og anviser også en række løsninger. Selvom fokus er på LoRaWAN, vil mange elementer i analyse og løsningsforslag også være relevante for kommuner, der har valgt at basere deres smart city løsninger på andre IoT-systemer, eksempelvis NB-IoT eller SigFox.

Fordel: Enheder kan arbejde asynkront

Smart city systemer baserer sig på sensorer og andre enheder i det offentlige rum. På grund af de fysiske afstande mellem enhederne er det ofte udelukket at benytte sig af kabler til kommunikation og strømforsyning. Kommunikationen skal derfor være trådløs, og strømforsyningen er ofte et batteri. Heldigvis er man typisk ikke afhængig af at kunne overføre store datamængder med høj hastighed og lav forsinkelse. Det åbner for, at man kan basere strømforsyningen på små batterier, der er billige og har lang holdbarhed. Desuden for, at man kan basere sig på trådløse kommunikationssystemer med lav båndbredde og lav pris. Bit-raten i disse systemer ligger sædvanligvis mellem 0,3 og 50 kbit per sekund. Altså væsentligt lavere end i bredbåndsløsningerne, som findes i mange husstande og virksomheder – her regner man i megabit. Disse "smalbåndssystemer" baserer sig samtidig på væsentligt lavere sendefrekvenser end bredbåndsløsningerne. Det mindsker energiforbruget – og giver stor rækkevidde som en bonus.

Smalbåndssystemerne giver mulighed for, at man lokalt kan skabe trådløse netværk. I Danmark er de mest udbredte lokale trådløse netværk LoRaWAN, Narrowband Internet-of-Things (NB-IoT) samt SigFox.

LoRaWAN er en såkaldt MAC-protokol (Media Access Control), som er udviklet af LoRa-alliancen, der har flere end 500 virksomheder og organisationer i en lang række lande som medlemmer. LoRaWAN definerer sendefrekvenser, overførselshastighed for data samt strømforsyning for alle apparater i systemet. Enhederne i netværket er asynkrone. Det vil sige, at de kan operere i hver deres rytme. Således er en sensor ikke nødt til at kommunikere med bestemte intervaller – den kan nøjes med at kommunikere, når den "har noget at fortælle". Et eksempel her er den kommunale skraldespand, der først melder sig, når sensoren registrerer, at det er på tide at tømme spanden.

Tillader datavalidering

Data fra en sensor eller tilsvarende enhed modtages af en forbindelses-enhed, en såkaldt packet forwarder, som sender datapakker videre til en central netværksserver. Netværksserveren kan filtrere pakkerne samt udføre sikkerhedskontrol og overordnet styring af netværket. Generelt har LoRaWAN-teknologien høj pålidelighed. Dog kan systemet have udfordringer med at sende automatiske bekræftelser på, at kommunikation er modtaget (signal receipt of message).

LoRaWAN benytter primært radio-frekvensbåndene 169 MHz, 433 MHz og 868 MHz. Fælles for disse bånd er, at de er licensfrie. Det vil sige, at båndene kan benyttes uden, at man er nødt til at betale teleskaber eller andre licenshavere.

Dette betyder dog også, at der kan opstå konkur-

rence om frekvensbåndet med andre i nærområdet, som måtte ønske at benytte LoRaWAN.

Grundlæggende består teknologien af to dele.

LoRa (Long Range) er den fysiske del. LoRa er en trådløs kommunikationsteknologi udviklet af virksomheden Cycleo, som i dag ejes af Semtech. LoRa har høj rækkevidde – længere end 100 km. LoRa forudsætter, at man holder bit-raten under 50 kbit per sekund. Der er også nogle andre begrænsninger. Systemet egner sig ikke til anvendelser, hvor man skal kommunikere i realtid eller hvor forsinkelser på signalet er uacceptable.

LoRaWAN er den software og hardware, som ligger oven på selve LoRa kommunikationssystemet. I LoRaWAN har man altid to servere – en netværksserver og en server til den enkelte tjeneste, applikations-serveren. Applikationsserveren kan forsyne andre systemer med den information, der sætter dem i stand til at styre kritiske funktioner – eksempelvis kontrol med togsystemer. Det er muligt at udstyre applikations-serveren med algoritmer, der udstyrer eksterne systemer med funktionalitet. Et eksempel er datavalidering, som er et vigtigt redskab for den, der vil overvåge systemet og sikre sig, at der ikke forekommer uregelmæssigheder – hvad enten det drejer sig om autoriserede eller uautoriserede handlinger.

Sikkerhed af netværksserveren er kritisk

DTU Compute's Hackerlab har analyseret forskellige risici i LoRaWAN.

Ifølge analysen er det især netværksserveren, som er sikkerhedskritisk i forbindelse med LoRaWAN. Netværksserveren håndterer de indkommende beskeder fra enhederne ude i byrummet. Denne server står også for at udføre sikkerhedstjek på den indkommende kommunikation samt for at videresende kommunikationen til den relevante applikations-server. Med andre ord er netværksserveren det led i systemet, som en angriber typisk ville udvælge som sit mål. Netværksserveren er sårbar over for alle typer af angreb, hvad enten man ønsker at plante bestemte falske observationer eller blot at "jamme" systemet og få det til at lukke ned. Derfor er den hyppigste forsøg på indtrængen, at angriberen først identificerer en sårbarhed enten i en bestemt enhed eller i kommunikationen mellem enhed-gateway-server. Denne sårbarhed forsøger angriberen derefter at udnytte til at omgå den sikkerhedskontrol, som er indbygget i netværksserveren.

Til gengæld er applikationsserveren mindre kritisk. Applikationsserveren er snarere det sted, hvor man konstaterer, at man har et problem, fordi serveren ikke trigger den aktion, som den burde, eller omvendt udløser en aktion, som ikke burde finde sted. Årsagen til dette ligger imidlertid typisk et andet sted end i applikationsserveren selv.

Endelig er der altid sårbarheder i selve de fysiske enheder – sensorer, forbindelsesenheder mv. Disse enheder kontrollerer de data, som bliver sendt i systemet. Et muligt problem er utilsigtede aktioner forårsaget af falsk input, mens et andet er mangel på aktion, fordi nogen har provokeret en fejl på systemet. Desuden kan en fysisk enhed være sårbar over for, at en angriber gensender beskeder, som enheden selv har genereret (replay attack) eller opsnapper informationer for at videresende dem til et andet device efter at have initieret kontakt selv i sammenhænge som datatransmission mellem gateway og server (relay attack). Endelig kan der være risiko for, at en angriber sender en besked af så lang varighed, at enheden ikke kan håndtere den og må lukke ned (jamming). Generelt er angreb på de fysiske enheder dog mindre kritiske end angreb på netværksserveren.

Typiske sårbarheder i LoRaWAN

I forbindelse med analysen har DTU Compute's Hackerlab gennemført en række simuleringer – "attack experiments" – hvor der er identificeret sårbarheder i et typisk LoRaWAN setup, og hvor det videre er forsøgt at udnytte de fundne sårbarheder til at forstyrre eller ødelægge systemet.

Resultaterne af analysen kan oversættes til en række krav til udbyderne af LoRaWAN-systemer.

Et godt krav er, at default setups for LoRa er: LoRa 1.1.x med 32 bit frame counter, OTAA (over the air activation), og over-the-air upgrade.

I forhold til netværksudbyder kan man med fordel bede om beskyttelse imod replay attacks i form af faulty packet detection algoritmer på netværksserver og/eller applikationsserver. Ydermere kan det være en god ide at oprette et privat netværk (VPN) med henblik på at undgå såkaldte rogue access points. Videre anbefaler vi fysisk beskyttelse på pins, busses og porte sammen med fejlsikring på de fysiske devices. Visse dataformater kræver desuden anonymisering i form af enten kryptering eller sløring (hashing).

I henhold til konfigurering er det værd at nævne brugen af spreading factor (SF). Det vil sige at sende den samme data-bit mere end en gang ved at sprede den, dvs. at multiplicere den med en

konstant kode. Dette sikrer en højere robusthed i kanalen. Spredningsfaktoren er ortogonal, hvilket betyder, at den samme frekvens kan bruges til at sende beskeder med forskellige spredningsfrekvenser uden, at de interfererer med hinanden.

Aktiver den indbyggede sikkerhed

Per default kommer LoRa med flere sikkerhedsforanstaltninger, som man enten selv kan konfigurere eller kan bede sin udbyder om at konfigurere. Det drejer sig blandt andet om end-to-end kryptering samt integreret beskyttelse mellem netværk og devices. Dette fungerer som en beskyttelse af fortrolighed – typisk som værn mod såkaldt sniffing – og som autorisering mellem netværk og device, samt beskyttelse mod manipulering af datapakker under transmission. Ydermere er det muligt at sikre LoRaWAN-netværket ved hjælp af integration af end-devices fra starten samt brug af MQTT-protokollen mellem gateway og LoRaWAN netværksserveren, hvilket nogle udbydere tilbyder. Integration mellem netværk og applikationsserver indgår indtil videre ikke som default mulighed, men dette bør indføres for at sikre kanalen med VPN eller lignende.

Desuden er det værd at overveje en række muligheder for at konfigurere firewalls samt metoder, der kan detektere angreb:

DevAddr: Device adresse med 4 byte værdi, som er en netværks-unik device-adresse i LoRaWAN svarende til en IP-adresse.

FCnt: Frame counter nummer, som er en 2 byte værdi med mindst 16 signifikante bits (LSB) af hele frame counteren, som har et felt, der øges med værdi 1 (inkremeres) med hver trasnsmission af pakker.

FRMPPayload: Dette er frame payload, som indeholder den faktiske krypterede LoRaWAN payload sendt fra end-device. Dens maksimale størrelse er givet ved den spread factor (SF) og båndbredde, som LoRaWAN er sat op med.

MIC: message integrity code er en 4 byte værdi, der fungerer som authentication regnet over hele pakken. Størrelsen af data-rate bestemmes af den maksimale længde af LoRaWAN-payload, applikations-payload og MAC-payload, hvilket også afgør sikkerhedskravene (MIC-værdien).

Endelig tilbyder LoRaWAN symmetrisk nøglekryptering med advanced ecryption standard (AES) med to 128 bits krypterings-nøgler, Network session key (NwkSkey) og applikations session key (AppSkey) i forskellige modes of operation i.e. counter (CTR) mode for kryptering og Cipher-based message authentication code (CMAC) for integritetsbeskyttelse. NwkSkey er delt mellem end-device og netværksserver, mens AppSkey er delt mellem end-device og applikationsserver. Der er to metoder, man kan bruge til at generere nøgler, som kan forveksles med autoriseret kryptering og dekryptering. Den første er Over the Air activation (OTAA), som kræver en joint procedure mellem netværk/applikationsserver og end-device.
Den anden er Activation by personalization (ABP), som er hard-coded nøgler til devices.

Muligt at konfigurere sikkerheden selv

Sammenfattende er det altså muligt at forbedre sikkerheden i LoRaWAN relativt enkelt ved at konfigurere en række værktøjer, der allerede ligger i systemet som default. Det skal noteres, at den konkrete konfigurering kommer an på, hvilken udbyder man har. Nogle løsninger indeholder simple grænseflader, hvor man nemt – med klik eller ved at indsætte tekst – kan konfigurere elementer som OTAA, indsættelse af detektionsmetoder, autoriserings-protokol mv., men dette afhænger igen af, hvordan udbyderen har sat systemet op. Her tænkes særligt på netværksserveren og applikationsserveren.

Det kan anbefales at implementere hele systemet internt, hvis man ønsker fuld frihed til sikkerhedskonfigurering. Alternativt kan man gå i dialog med sin udbyder om de mest presserende konfigureringer:

// **Brug LoRa 1.1.x:** Denne version indeholder en 32-bit frame counter, hvilket gør replay attacks sværere. Dette er en forbedring i forhold til LoRa 1.0.x. Sørg for at system og devices kører på 1.1.x versionen før anskaffelsen.
// **Forebyggelse af jamming:** Brug af flere gateways gør jamming svært, da angriberen vanskeligt kan lokalisere, hvilket af flere "forwarder points", som skal rammes.
// **Detektionsmetoder:** Som script kan indsættes forskellige detektionsmetoder i netværksserveren eller applikationsserveren. Metoderne bygger på analyse af data i systemet – eksempelvis krydsvalidering, dyb læring, machine learning etc. – med det formål at fange falske datapakker. Man kan implementere detektion selv eller hyre ekstern hjælp.
// **Tidsinformation i datapakker:** Ved at indsætte information om tidspunkter i datapakkerne kan man sikre sig friskhed og dermed forebygge mange såkaldte replay-angreb, hvor angriberen benytter sig af opfangede gamle beskeder. Snak eventuelt med din udbyder eller direkte med LoRa.
// **Autorisering:** TCP handshakes med en tre-trins metode, der kræver at klienten og server udveksler SYN (SYNchronize) og ACK (acknowledgements) pakker før udveksling af faktiske datapakker og kommunikation begynder. Brug af signatur og hemmelige nøgler kan yderligere forstærke krypteringen. Dette skal gøres på netværksserverdelen af systemet. Dette er specielt vigtigt for kommunikation mellem applikation og netværksserver, da det ikke er indbygget som default. Tag en snak med udbyderen om mulighederne.
// **OTAA (over the air activation):** Dette er en langt mere sikker løsning end alternativet, som er activation by personalization, da OTAA har en fælles procedure inkluderet.
// **Hardware sikkerhed:** Der findes en række fysiske sikkerhedsenheder beregnet til såvel gateways som devices. Eksempelvis særligt sikre chips (fail-safe chips) og sensorer samt afskærmning af pins og porte, fysiske låse, forebyggelse af side-kanal angreb, sletning af private nøgler ved indtrængen mv. I bund og grund handler det om at tage en snak med sin leverandør om mulighederne.
// **Sikkerhedskultur:** Medarbejdernes adfærd er naturligvis en vigtig faktor i forbindelse med smart city sikkerhed. Det er vigtigt at gøre opmærksom på risikoen for phishing og andre tilsvarende typer af angreb.
// **Løbende opdatering og vedligehold af servere:** Dette er vigtigt at etablere, herunder at man har producerer, der fastslår frekvensen af opdateringer samt hvem, der har ansvaret. Dette omfatter også sletning af data mv.
// **Beskyttelse af servere:** Vigtigt at etablere sikkerhed af server og webapplikationer, så disse beskyttes mod malware og virus.
// **Høj datarate:** Dette kan beskytte mod en del usikkerheder relateret til Denial-of-service.

Sikkerhedsanalysen, som DTU Compute's Hackerlab udførte af LoRaWAN for Smart City Cybersecurity Lab, gennemgås nærmere i håndbogens tekniske sektion.

Lad dig hacke af DTU!

Smart City Cybersecurity Lab har været med til at etablere Hackerlab på DTU Compute. Kommuner og andre, der arbejder med smart city systemer, er velkomne til at henvende sig til Hackerlab. Laboratoriet har for eksempel mulighed for at lade studerende forsøge sig med at hacke dit system (såkaldt "white hat hacking") og på den måde afdække sårbarhederne i systemet.

Vær dog opmærksom på, at laboratoriet ikke fungerer som et privat konsulentfirma, men er baseret på dygtige studerende, som ønsker at lære om sikkerhed uden dog at have de værktøjer og erfaringer, man normalt forventer af en konsulentvirksomhed. Aktiviteten følger rytmen i undervisningen på DTU. Således skal større eksterne samarbejdsprojekter passe med semesterstart, dvs. påbegyndes enten i januar eller august. Af hensyn til planlægningen er det tilrådeligt at henvende sig nogle måneder før projektet tænkes påbegyndt, altså midt på foråret eller midt på efteråret. Projekterne kan typisk have en tidshorisont på tre-seks måneder.

Hackerlab på DTU svarer gerne på spørgsmål, men vær i god tid med ideer til samarbejdsprojekter.

Du kan læse mere på http://www.hackerlab.dtu.dk/

/ Pas på kronerne og undgå røde ører /

Sikkerhedssoftware er som regel billig. Men det er konsulenttimer ikke.

Enhver, der vil starte et nyt smart city projekt, bliver hurtigt mødt med spørgsmålet om, hvad det koster. Økonomi er altid en vigtig faktor i forbindelse med offentlige projekter.

Det falder imidlertid uden for formålet med denne håndbog at opgive eksakte priser på de forskellige løsninger inden for cybersikkerhed. Selv hvis vi forsøgte os, ville oplysningerne være forældede meget hurtigt, fordi trusselsbilledet og de tilsvarende løsninger hele tiden ændrer sig.

Hvad angår omkostningerne til den hardware, som benyttes i smart city systemer, kan vi henvise til guiden "Den smalle digitale revolution" udgivet af smart city samarbejdet Gate 21 i december 2018. Guiden, som er offentligt tilgængelig for download, giver en oversigt over typisk hardware i smart city systemer. Desuden er de omtrentlige priser for de forskellige typer af hardware angivet – naturligvis med forbehold for, at markedet for smart city systemer er i konstant udvikling.

Ud over standard hardware som sensorer, servere m.v. kan det ofte være fornuftigt at indsætte særlig hardware, der øger sikkerheden. Nærmere detaljer omkring sådan sikkerhedshardware kan læses i håndbogens tekniske sektion.

Få styr på ansvaret i driftssituationen

Hvad angår software, kan vi sige helt generelt, at udgiften til selve den sikkerhedssoftware, som man skal benytte, typisk er lille set i forhold til det samlede budget for smart city projekter. Ofte kan man få den relevante software som Open Source. Til gengæld kan det hurtigt blive dyrt alligevel, hvis man er afhængig af eksterne konsulenter til at analysere trusselbilledet og stå for at installere software.

I den sammenhæng er det særdeles vigtigt, at man ikke kun har øje for, hvad systemet koster i anskaffelse. Ved valget af sikkerhedsløsninger er det helt afgørende, at man beslutter sig for, hvordan løsningerne skal opdateres, når systemet kommer i drift. Hvem har for eksempel ansvaret for, at de uundgåelige opdateringer – såkaldte patches – som kommer fra leverandørerne, faktisk bliver installeret? Og hvem har ansvaret for at tjekke, at systemer til anonymisering af personoplysninger faktisk bliver implementeret, og at oplysninger, som ikke længere er nødvendige, faktisk bliver slettet?

Ikke mindst i forbindelse med pilotprojekter er det også vigtigt, at man tidligt afklarer, hvordan ansvaret for disse sikkerhedsprocedurer skal varetages på et senere tidspunkt, når man går over til fuld drift.

Sæt tal på din sårbarhed

Behovene for sikkerhed varierer i forhold til, hvilket formål systemet har. Et eksempel på et system er målere af vandstande. Her vil det typisk være andre forhold – driftssikkerhed, lang levetid af batterier mv. – der er afgørende i forbindelse med indkøbet og opsætningen.

To gode metoder til at klassificere sårbarheder er henholdsvis CVSSv3 (Common Vulnerability Scoring System, version 3) og CWSS (Common Weakness Scoring System). Begge scoringsmodeller bygger på estimering og kan bruges sammen med modeller til korrelation (fx CAPEC-modellen), der har kortlagt en del angrebsmønstre. Derved er det muligt at få en numerisk evaluering – eventuelt ved at inddrage ekspertise inden for cybersikkerhed - af sikkerheden i et IoT-system.

Fordelen ved at evaluere sikkerheden numerisk med et scoringssystem er, at man derefter kan lægge resultaterne ind i scenarie, hvor omkostningerne ved at sikre sig er vejet op mod konsekvenserne, hvis det går galt. Med andre ord: er de mulige tab og graden af sårbarhed så alvorlig, at jeg vil påtage mig de investeringer, som det koster at gardere sig?

/ Mere om teknikken bag smart city sikkerhed /

Denne sektion er for dig, der ønsker at komme et spadestik dybere ned i de tekniske aspekter omkring kortlægning af trusler samt sikkerhedsløsninger. Arbejdet er udført af DTU Computes Hackerlab i regi af Smart City Cybersecurity Lab og projektet Safer Copenhagen.

Et typisk smart city system – eller IoT-system, dimsernes internet – er bygget op i fem niveauer.

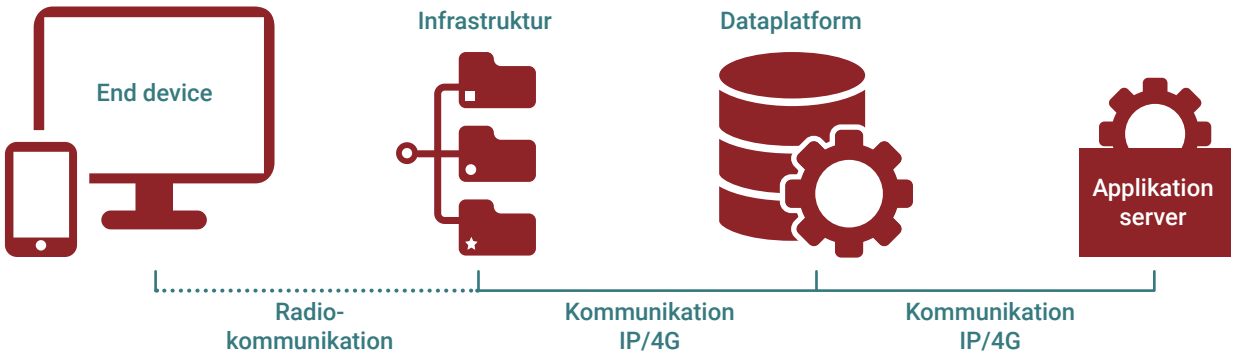
Længst ude i systemet har man et antal sensorer, kameraer eller tilsvarende enheder. Dette niveau kaldes "end devices".

Næste niveau er "infrastruktur". Det vil sige udstyret, der står for at indsamle og transmittere de data, som indsamles fra end devices.

"Data-platformen", som modtager og behandler rådata, er et centralt niveau i systemet.

Fjerde niveau er "applikations-serveren". Denne server fodres med behandlede data fra data-platformen. Applikationsserveren er dedikeret til det særlige formål, som projektet skal tjene – for eksempel inden for trafikregulering, affaldshåndtering eller andet.

Endelig er det sidste niveau "kommunikation". Det kan for eksempel være afsendelse af kommandoer ud til end devices eller til andre systemer i en kommune.

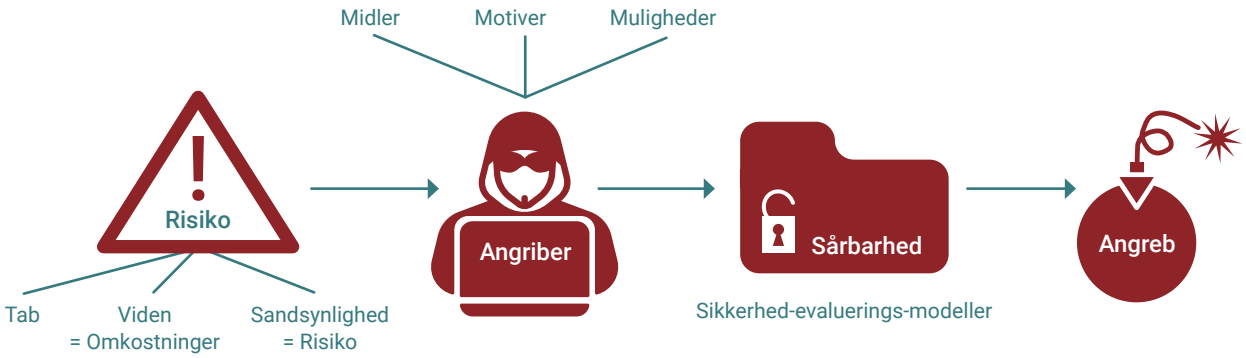


Kortlæg angrebsfladerne i systemet

Udgangspunktet for sikkerhedsvurdering af systemet vil altid være en kortlægning af de mulige angrebsflader på de fem niveauer.

For hver angrebsflade vil der være et antal trusler. Det er muligt at opstille analysen som et hierarki med angrebsflader øverst, dernæst de tilhørende trusler – og for hver trussel videre en forsvarsteknik samt en testmetode, der kan afprøve effektiviteten af forsvaret. Videre bør analysen have to yderligere lag: Hvad er konsekvensen, hvis det alligevel lykkes for en angriber at trænge igennem forsvaret? Og hvilke tiltag skal man sætte i værk for at kunne genoprette systemet?

Denne model benyttede DTU Computes Hackerlab til analysen af sikkerhed i LoRaWAN-systemet:



Ud fra den overordnede model opstillede Hackerlab en række mulige tab (losses), farer (hazards) og kontrolaktioner i forbindelse med LoRaWAN:

// Tab:
  // Skade på LoRaWAN
  // Skade eller tab på kritiske systemer
  // Skade på den offentlige sundhed
// Farer:
  // Ukontrollerede/ukorrekte data
  // Ukontrollerede transmissioner af data
  // Komponentfejl
// Kontrolaktioner
  // Send data
  // Mellem applikationsserver og LoRaWAN (Start/stop, øge/begrænse, omdigirigere etc.)

De vigtigste anbefalinger på baggrund af analysen er nævnt i håndbogens kapitel "Overvejelser om sikkerhed i LoRaWAN".

Komponent-for-komponent-tilgangen

Naturligvis er det også muligt at benytte en mere traditionel tilgang, hvor man ser på de forskellige komponenter i smart city systemet en for en. Der findes en række online fællesskaber – eller communities som det hedder på nudansk – hvor medlemmerne kollektivt samler erfaringer omkring cyber-sikkerhed i forbindelse med bestemte typer af komponenter. Her kan man få viden om angrebstyper og sårbarheder samt virkemidler til at sikre komponenterne.

Et fællesskab med høj troværdighed er OWASP, som blandt andet vedligeholder og opdaterer en liste over trusler mod IoT-systemer: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.

Et andet værdifuldt fællesskab er CWE (common weakness enumeration). Efterhånden, som nye angrebsmetoder og sårbarheder viser sig, tildeles de et nummer i CWE's klassifikation. Ideen er at gøre det lettere for brugerne at finde de forebyggende strategier i forhold til de pågældende trusler.

Høj bit-rate, bedre sikkerhed

En nøglefaktor for sikkerheden i smart city systemer er hastigheden i datatransmissionen. Denne hastighed, som måles i bit-rates, er afgørende i situationer, hvor det er lykkedes en udefrakommende at trænge ind et sted i systemet. Dette kaldes i fagjargonen "man-in-the-middle" angreb.

Jo højere bit-rate, jo mere sikkert er systemet. Fx anbefaler DTU Computes Hackerlab, at man mindst har 32 bit frame, hvis man baserer sig på et LoRaWAn smalbåndssystem.

Desuden er det vigtigt at være opmærksom på certificeringer og ejerskab af data, når man indkøber teknologi til fremme af cybersikkerheden ved smart city systemer. Nærmere bestemt bør man spørge ind til ejerskab, håndtering og vedligeholdelse af de komponenter, der følger med, med hensyn til datalagring, hardware, firmware, kommunikation, tjenester, servere, netværk og applikationer/dashboard.

Andre krav, som man bør stille, angår håndteringen af data. Som minimum bør datapakker være krypteret, og man bør sikre sig, at transmissionen foregår over sikre kanaler. Dette kan eksempelvis ske ved, at man etablerer et VPN (virtual private network). Et VPN udstrækker et privat netværk over et offentligt netværk. Med andre ord kan brugere, der er autoriserede til at deltage i netværket, logge på over et offentligt netværk med deres passwords og have samme niveau af sikkerhed, som hvis de var logget på inde på det private netværk.

Efterspørg friskhed i datapakker

Et andet godt spørgsmål at stille er, om leverandøren tager højde for friskhed (freshness) i datapakker. Hvis man ikke har denne faktor indbygget, vil det være muligt for en angriber, der har opsnappet kommunikation i systemet, at gensende gamle datapakker og få systemet til at tro, at der er tale om ny kommunikation. En del leverandører glemmer at indbygge freshness i deres løsninger.

Endelig bør man sikre sig, at anerkendte standarder overholdes. For mange typer af udstyr og systemer til smart city anvendelser findes der etablerede standarder. Det gælder fx de såkaldte Top 20 telco standards. Eksempler er ISO 27000 serien (information security management), ISO 31000 serien (risk management), ISACA COBIT 5, NIST SP 800 – 61 (computer security incident handling guide) samt PCI DSS (payment card industry data security standard). Ydermere kan man benytte best practice-modellen TVM til pen-testing, sårbarhedsskanning, vurdering af web-applikationer samt teknisk konfigurering sikkerhedsvurdering.

Det er vigtigt at få stillet spørgsmålene forud for den egentlige aftaleforhandling og implementering af systemet.
I den forbindelse er det desuden altid en god ide at efterspørge en demonstration af sikkerheden.

Ekstra beskyttelse til kritisk infrastruktur

I forhold til kritisk infrastruktur som eksempelvis kontrol med trafiklys anbefaler DTU Compute's Hackerlab, at systemet beskyttes med fysiske switches, challenge/response protokoller samt bluetooth-style fjernkontrol. Nærmere bestemt kan hardware sikres ved hjælp af switches, der lukker en enhed, som er kompromitteret, ned. Desuden bør styringen af trafiklysene være udstyret med verifikation af krypteret kommunikation, programmerbare nedluknings-mekanismer, integrerede kredsløb, beskyttet UART (Universal Asynchronous Receiver-Transmitter), samt el-kabler sikret mod indtrængen/forstyrrelse via nabo-kabler. Videre bør den boks, som rummer trafiklysets kontrolpanel, være beskyttet med en mekanisme – såkaldt tamper protection – som sørger for, at panelet lukker ned, hvis boksen, hvor panelet sidder, er åbnet uden brug af systemnøglen. Desuden bør trafiklysene være isoleret i forhold til hinanden. Med andre ord skal det ikke være muligt at tilgå andre trafiklys digitalt for en indtrængende, som er lykkedes med at nå ind i styringen af et enkelt trafiklys. Endelig bør kommunikation i systemet ske ved hjælp af VPN. De nævnte løsninger er relevante i en lang række smart city systemer.

Stil de rigtige spørgsmål om dit system

Ud over den hierarkiske model og komponent-for-komponent-tilgangen findes der en tredje måde at forholde sig til cyber-sikkerhed i smart city systemer. Denne tredje tilgang adskiller sig fra de to andre ved, at man stiller en række fundamentale spørgsmål, som ikke knytter sig til de konkrete komponenter i systemet. Derved egner denne model sig som et supplement til de to øvrige tilgange. Spørgsmålene knytter sig til tre hovedtyper af angrebsflader:

// **De fysiske angrebsflader** – sensorer, data porte, kommunikation mellem system og bruger, fysiske adgangsbarrierer (døre, som er låst med nøgler eller kodede alarmsystemer mv.), chips, hardware generelt.
// **Angrebsflader i software** – apps, web-sider, firmware.
// **Angrebsflader i kommunikationen** – kommunikation over internettet, radiokommunikation (typisk over smalbånd).

Spørgsmål til de fysiske angrebsflader:

Hvordan aflæser systemet data?
// Kan vi manipulere sensorerne, så de producerer forkerte data?
// Hvor godt er systemet i stand til at håndtere en hurtig strøm af indkommende data?

Kan man angribe via nærliggende datakanaler (side-channel attacks)?
// Er systemet udstyret med adgangskontrol, som stopper falske data?
// Er der ubeskyttede adgangsveje?
// JTAG eller UART?

Hvilke data bliver lagret i hukommelsen?
// Hvordan tilgår man disse data?
// Kan man manipulere data, der er lagret i hukommelsen?

Hvordan bliver end devices opdateret?
// ABP eller OTAA?

Hvordan bliver leverandør-software (firmware) installeret?

Spørgsmål til software:

Er der sårbarheder i de anvendte biblioteker?

Er der ubenyttede funktionaliteter i softwaren?
// Hvordan aktiveres ubenyttede funktionaliteter?

Hvor lagres data?

Hvordan er adgangen til lagrede data?

Hvordan kan lagrede data ændres?

Hvordan bliver input renset?
// Er det muligt at indføje aktive programmer?

Spørgsmål til kommunikationen:

Er der sårbarheder i kommunikationsprotokollerne?
// Hvilke værdier findes i http-overskriften?

Er der "friskhed"?
// Har man ikke indbygget friskhed, vil det være muligt at gensende gamle data ind i systemet (replay attack).

Er dele af kommunikationen uden kryptering?
// Hvilke informationer kan man få fra denne ikke-krypterede kommunikation?
// Kan vi udnytte disse informationer til at skabe vores egne datapakker, som systemet vil opfatte som genereret af systemet selv?

Er det praktisk muligt at knække kryptering?
// Ved hjælp af rå datakraft?
// Ved hjælp af en digital ordbog?

Er protokollen symmetrisk?

Er det muligt at nedgradere protokollen til en protokol med svagere beskyttelse?

Er der sårbarheder i de udbudte tjenester? Hvordan bliver komponenter og brugere føjet til systemet?

Hvordan er adgangskontrollen (autoriseringen) for brugerne?

Er det muligt at finde frem til brugernavne?

Er informationer om passwords tilgængelige for brugere uden autorisering?
// Kan vi finde informationer om brugerne gennem systemet? For eksempel hints om passwords eller spørgsmål, der kan hjælpe med at genskabe passwords?
// Kan autoriseringen knækkes ved hjælp af rå datakraft inden for en praktisk tidshorisont?
// Kan vi opnå hel eller delvis adgang? Som bruger? Som end-device? Er det muligt at tilegne sig yderligere rettigheder, når man har opnået en sådan begrænset adgang?

Specifikationer for LoRaWAN, SigFox, NB-IoT

Som nævnt tidligere i håndbogen har en del danske kommuner valgt at basere smart city løsninger på smalbåndskommunikation over LoRaWAN. Generelt kan man sige, at LoRaWAN egner sig bedst til smart city systemer, hvor der bliver sendt relativt små datapakker og hvor det ikke gør så meget, at man noget forsinkelse i transmissionen. Eksempelvis data fra sensorer, der måler mængden af affald i en skraldespand eller vandstanden i en å. Ønsker man derimod real-tids opdateringer, er et system som NB-IoT mere relevant grundet større datakapacitet og hurtigere transmission. Tabellen her sammenligner de tekniske specifikationer for de tre smalbånds-systemer, som dominerer det danske IoT-marked.

Aspect	LoRaWAN	SigFox	NB-IoT
Uplink data rate	> 50 kbps	0.1 kbps	> 170 kbps
Downlink data rate	> 50 kbps	0.1 kbps	> 250 kbps
Indoor penetration	+20dB	+13dB	+9dB
Gateway independent	Ja	Nej	Nej
Licensed spectrum	Ja	Nej	Nej
Frequency Bands	863-870 MHz	Uplink: 868.034-868.226 MHz Downlink: 869.4 - 869.65 MHz	LTE Licens bånd
Duplex	Half-duplex, FDD	Half-duplex, FDD	Half-duplex, FDD
Modulation	LoRa/FSK	Uplink: D-GPSK Downlink: GFSK	Uplink: BPSK/QPSK Downlink: QPSK
Diversity Scheme	Chirp Spread Spectrum, Uplink Spatial diversity	Uplink: Time, Frequency, and Spatial Diversity	Time Diversity
Multiple Access	ALOHA (random acccess)	ALOHA (random access)	Uplink: SC-FDMA Downlink: OFDMA
Bandwidth	125/250/500 kHz	Uplink: 100 Hz Downlink: 600 Hz	Uplink: 3.75-180 kHz Downlink: 15-180 kHz
Max. Tx Power	Uplink: 14dBm Downlink: 27dBM	Uplink: 14dBm Downlink: 27dBm	Uplink: 23dBM Downlink: 43dBm
Bit rate	250bps-50kbps	Uplink: 100bps Downklink: 600bps	20-250kbps
Max payload size	242 bytes	Uplink: 12 bytes Downlink: 8 bytes	1599 bytes
Payload encryption	AES128 CTR	Optional AES128 CTR	128bit EEAx
Control encryption	Nej	Nej	Ja
Authentication	Device and Network	Device and Network	Device and Network
Frame integrity	4 bytes MIC	2-5 bytes MAC	4 bytes MAC or None
Replay protection	16/32 bit frame counter	12 bits sequence number	32 bits COUNT value
Session Key updatability	Mulig	Nej	Mulig
Reliable Delivery	Begrænset	Begrænset	Mulig
OTA firmware update	None	None	Mulig
Jamming	Sårbar	Sårbar	Sårbar
Sniff-replay	Sårbar	Sårbar	Ack delivery sårbar
Replay attack	Ikke sårbar for 1.1.x Sårbar for 1.0.x 16 bit Frame counter	Sårbar efter X antal pakker	Ikke sårbar for data over NAS eller kontrol data over AS men sårbar overfor data over AS
Packet forging	Sårbar for bruteforce med 4 byte MIC hvilket er meget svært	Sårbar Bruteforce MAC	Sårbar for data over NAS med bruteforce 4 byte MAC (meget svært). Sårbar user data over AS.

LTE Bånd nummer	Uplink frequency (MHz)	Downlink frequency (MHz)
1	1920 - 1980	2110 - 2170
2	1850 - 1910	1930 - 1990
3	1710 - 1785	1805 - 1880
5	824 - 849	869 - 894
8	880 - 915	925 - 960
12	699 - 716	729 - 746
13	777 - 787	746 - 756
17	704 - 716	734 - 746
18	815 - 830	860 - 875
19	830 - 845	875 - 890
20	832 - 862	791 - 821
26	814 - 849	859 - 894
28	703 - 748	758 - 803
66	1710 - 1780	2110 - 2200

Tech	Frequency	Data Rate	Range	Power Usage	Cost
2G/3G/4G	Tele bånd	10 Mbps	Par Kilometer	Højt forbrug	Høj
Bluetooth/BLE	2.4 GHz	1,2,3 Mbps	~ 100 meter	Lavt forbrug	Lavt
IEEE 802.15.4	subGHz,				
2.4 GHz	40, 250 kbps	> 260 Km2	Lavt forbrug	Lavt	
LoRa	subGhz	< 50 kbps	1-5 Km	Lavt forbrug	Middel
LTE Cat 0/1	Tele bånd	1-10 Mbps	Par Kilometer	Middel forbrug	Høj
NB-IoT	Tele bånd	0.1-1 Mbps	Par Kilometer	Middel forbrug	Høj
SigFox	subGhz	< 1 kbps	Par Kilometer	Lavt forbrug	Middel
Weightless	subGhz	0.1-24Mbps	Par Kilometer	Lavt forbrug	Lavt
Wi-fi	subGhz, 2.4Ghz, 5GHz	0.1-54 Mbps	< 100 meter	Middel forbrug	Lavt
WirelessHART	2.4 GHz	250 kbps	~100 meter	Middel forbrug	Middel
ZigBee	2.4 GHz	250 kbps	~100 meter	Lavt forbrug	Middel
Z-Wave	subGhz	40 kbps	~32 meter	Lavt forbrug	Middel

Kilde: Helium Blog.

/ Vigtige begreber i smart city sikkerhed /

Begreb	Forklaring
Anonyme data og anonymisering	**Anonyme data er** data hvor man ikke kan genkende personer ud fra oplysningerne – heller ikke i kombination med andre oplysninger. Anonyme data er ikke underlagt persondataforordningen. Anonymisering er en vigtig øvelse i forhold til at kunne indsamle vigtig og brugbar information om personer. Øvelsen er ofte ikke triviel.
Anonymiseringsmetoder: Pseudonymisering og aggregering	**Pseudonymisering** kan defineres som "en behandling af personoplysninger, hvor personoplysningerne ikke længere kan henføres til en bestemt person uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk persondefineret" (kilde: Datatilsynet). Så længe pseudonymsiering foregår som ovenstående, vil den sikre borgeren anonymitet. Ved **aggregering** samler man oplysninger i grupper, så der ikke er fokus på et enkelt individ. Det kan f.eks. være et antal personer inden for et geografisk område. Aggregerede oplysninger er alene anonyme, såfremt personerne ikke kan genkendes ud fra oplysningerne eller ved at kombinere andre oplysninger med de aggregerede.
Challenge/response protokoller	I forhold til autorisering handler disse protokoller om adgang via en randomiseret challenge (et tal), der skal besvares fra klienten via en secret key. Resultaterne af challengen bliver sammenlignet mellem netværk og klient, og hvis de stemmer overens, er der adgang.
Devices i smart cities	Sensorer og lignende devices, der indsamler data og sender data.

Hacking.
 	
Forskellige typer af hacking:
	Radio hacking
	// Hacking fokuseret på radiofrekvenser inklusive jamming, replay attack, sniffing etc.
	
	Web hacking
	// Hacking af webapplikationer, der kan opnås via diverse WiFi auditing redskaber og angreb som phishing, cross site scripting og DOS.
	
	Hardware hacking
	// Fysiske angreb på devices, der fokuserer på porte, chips, firmware etc. inkl. Side-channel angreb.
	
	Database hacking
	// Et angreb specifikt fokuseret på databasen.
	
	Server hacking
	// Et angreb fokuseret på at inficere klienten og/eller hosten med den formål at opnå uautoriseret adgang til datapakker eller systemet.

Infrastruktur	Infrastruktur er den ramme i form af fysiske og digitale komponenter, man bygger systemer op af med henblik på at sikre flow, lagring, behandling og analyse.
ISO-standarder	En ISO-standard er en standard etableret og anerkendt af den internationale organisation for standarder.
IT og forretnings-arkitektur	Forretnings- og IT-arkitektur er fundamentet for at skabe en systematisk sammenhæng mellem forretningen og IT og for at opnå en bevidst styring af IT-sammenhænge og investeringer. Arkitektur-arbejde skal blandt andet sikre, at data kan flyde sikkert rundt i relevante systemer og genbruges i andre fremtidige brugssituationer.

Begreb	Forklaring
Kryptering	En teknisk foranstaltning, der sikrer at data ikke er umiddelbart læsbare, men skal låses op med den korrekte krypteringsnøgle. Kryptering bliver brugt, når man ønsker at beskytte personoplysninger eller kommunikation. Krypterede personhenførbare oplysninger er stadig at betragte som person-oplysninger, da krypteringsnøglen giver adgang til data. Krypterede data er derfor beskyttet af persondataloven.
Numerisk evaluering af sikkerhed	Standardiserede scoringssystemer, der evaluerer sikkerheden af systemer og devices på en skala, der tager parametre som hyppighed og lethed af kompromittering, sårbarhed, vigtighed og konsekvenser i betragtning.
Patches	Et fix, udbygning eller update til eksisterende software.
"Person reindentification"	En metode, hvor sammenstilling af data kan føre frem til oplysninger om et enkelt individ. En central problemstilling inden for smart city. Et eksempel er en kommune udstiller 4 datasæt, som hver for sig er anonyme, men ved at kombinere data, kan man personidentificere folk, der optræder i datasættet.
Privacy by design (PbD)	Privacy by design er et koncept, der integrerer beskyttelsen af personoplysninger i designfasen af systemer. Det er et krav, at nye løsninger med følsomme person-oplysninger er udviklet vha af Privacy by design principper. Brugernes adgangs-begrænsning til data nævnes ofte som et eksempel på et princip på privacy by design.
Realtidsdata	Realtidsdata er data, der er tilgængelig direkte efter de er indsamlet. Eksempelvis kan positionen for plæneklipper, droner og biler overvåges i realtid og overføres til et planlægningsværktøj. Kommunerne efterspørger mere og mere denne type data, og i fremtiden vil flere og flere automatiske handlinger blive foretaget på realtidsdata. Det kræver stort fokus på sikkerhed og privacy.
Risikovurdering	En risikovurdering fokuserer typisk på et konkret område eller et bestemt system. Den giver overblik over sandsynligheden for og konsekvenserne ved sikkerheds-brud på fortrolighed, integritet og tilgængelig, herunder mulige konsekvenser for organisationens omdømme. I forbindelse med risikovurderingen præciseres virksomhedens mål og risikovillighed. For hvert område vurderes en række mulige forbedringer og deres sikkerhedsmæssige konsekvenser.
Security by design	Et koncept, hvor du arbejder med allerede i designfasen af et system at indtænke sikkerhed.
Server	En server er grundlæggende en computer-ressource, der kan deles mellem autoriserede brugere (kaldet klienter) i et net. Det kan bl.a. bruges til lagring af data eller til kommunikation med andre operatører i et netværk.
Sikkerhedsanalyse	Sikkerhedsanalysen er en analyse af IT-tekniske trusler og sårbarheder i løsning og set-up rundt om den (nogle steder også kaldet for eksempelvis en teknisk risikovurdering eller cyber-sikkerhed).
Standarder	I sikkerhed er en standard en anerkendt måde at certificere sikkerheden i udstyr eller en bredt anerkendt konvention brugt af et system for sikker styring.
Switches	Switches er kontakter, der forbinder dit netværk til diverse devices, klient-porte osv. I forhold til sikkerhed er det vigtigt at inkludere Embedded security i netværket, Access control lister for adgangskontrol og virtual LANs for segmentering af grupper med autoriseret adgang.

ISBN nr.: 978-87-971357-1-6