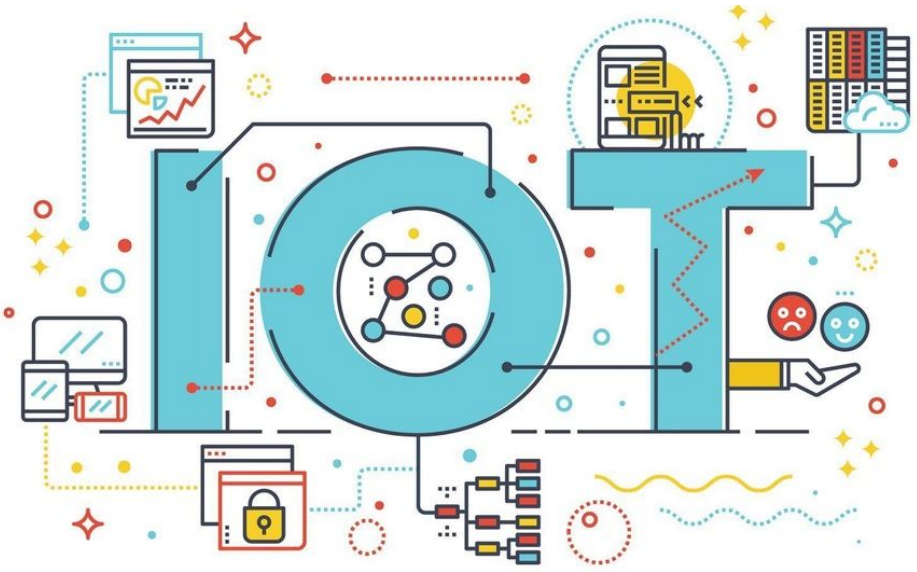
27-05-2019

# IoT-sikkerhed

## I et organisatorisk perspektiv




| |
|---|
| Eksamensgruppe nr: S1925625035 |
| Frederik Nicolai Høigaard Rasmussen - 60684 |
| Magnus Balling Engelsen - 61214 |
| Mikkel Schreiner - 61356 |
| Vejleder: Troels Andreasen |


Humanistisk-teknologisk bachelorprojekt

# Abstract

With the use of an organizational perspective, this study examines the security problems that relate to IoT environments. By combining the two methods of literature review and semi-structured interviews, we have been able to gain knowledge from previous studies and obtain new knowledge from interviews. This report aims to provide a trustworthy and righteous picture of the organizational IoT security issues that appear worldwide. Furthermore, this study attempts to outline the risk factors that companies may experience, as well as propose solutions to the subject. The study discusses the necessity of new guidelines in the landscape of IoT security, and concludes that a general need for international IoT security standards exist, which subsequently will support the global market competition. Ultimately, the study concludes that organizations experience problems regarding the complexity of IoT environments.

# Indholdsfortegnelse

# Begrebsafklaring

*Kryptering* - Indholdet af et datasæt gøres ulæseligt ved hjælp af en algoritme. En specifik nøgle kræves for at gøre materialet læseligt igen.

*White hat hacker* - Etiske hackere der udelukkende infiltrerer systemer for at identificere sårbarheder, samt undersøger om IT-sikkerheden er tilstrækkelig hos en given virksomhed.

*Operationel teknologi (OT)* - Hardware og software som detektere eller foretager ændringer i fysiske processer ved direkte overvågning eller kontrol af fysiske enheder, som f.eks. pumper, ventiler, varmestyring osv. (Trend Micro, 2018; 2).

*Endepunkter* - oversat fra det engelske ord "endpoints". Et endepunkt er en computerenhed som kommunikere med det netværk som den er tilknyttet. Eksempler på endepunkter er: bærbare- og stationære computere, servere, sensorer, printere m.m.

*Bots*: En større mængde af computere som en angriber har overtaget og bruger til ondsindede angreb.

*TCP/IP:* Transmission control protokol/internet protokol.

*SQL:* Structured Query Language. Programmeringssprog til databaser.

*Hardcoded adgangskoder:* Producenten har fastlåst en adgangskode til produktet, som ikke kan ændres.

ISO27001: International standard til etablering af et ledelsessystem for informationssikkerhed (Digitaliseringsstyrelsen, 2019)

# Indledning

Den øgede digitalisering gennem de sidste årtier har ført mange nye innovationer og tendenser med sig. Nogle har udviklet sig i en sådan grad at det kan være svært at tænke tilbage på en tid før disse teknologier, mens andre har været døgnfluer som igen er blevet glemt. En ting er dog sikkert; digitaliseringen og de medfølgende teknologier udvikles og udbreder sig hurtigere end nogensinde før. Den første innovation, som for alvor satte skub i digitaliseringen var internettet. Det skabte en helt ny platform for digitaliseringen, hvorpå internettet blev en kommunikationskanal for alle forbundne enheder. Efterhånden som flere og flere enheder blev forbundet til hinanden via netværk, øges mængden af data også i stigende grad. I en rapport fra Gartner Inc., forventes det at man i 2020 på globalt plan vil have op imod 20 milliarder forbundne enheder (Gartner Inc, 2017). Mange virksomheder finder denne udvikling interessant og vælger derfor at investere i *Internet of Things* (IoT). Når organisationerne påbegynder IoT-projekter, udsætter de sig for risikoen fra et udefrakommende cyberangreb pga. en øget antal endepunkter. Endepunkterne kan anvendes som et redskab til at infiltrere virksomhedernes netværk, for at få adgang følsomme data, overtage styringen af virksomhedens computer, eller sabotere netværk. I takt med den øgede mængde af forbundne enheder, både hos forbrugere og hos virksomheder, har det medført et stigende behov for IT-sikkerhed og databeskyttelse (Mediernes udvikling, 2015). De mange forbundne enheder betyder en større kompleksitet i IT-infrastrukturen hos virksomheder, som derfor er mere sårbare overfor angreb. Det er dog ikke nemt for virksomheder at sikre deres data og det er dermed en problematik der bør tages alvorligt.

# Motivation

Nysgerrighed er ofte et helt centralt element, når nye studier bliver til. Nysgerrighed er den drivende faktor for et projekt og det er med til at skabe motivation for projektets dannelse. Motivationen for dette projekt bygger til dels på en fælles interesse for genstandsfeltet, samt flere kurser der har åbnet op for feltets mange problematikker. Noget af det som vi finder allermest interessant er de mange muligheder og fordele som IoT giver virksomheder, samt de forhindringer sikkerheden medfører. Et andet element i motivation, er de mange læringsrige oplevelser der opstår i løbet af en projektperiode. At videreformidle begreber og teorier i en forståelig kontekst kan være en udfordring, men det er netop dét, som også gør et projekt spændende og udfordrende at arbejde med. Det er også med til at

skabe en vedvarende motivation, som i sidste ende vil være en katalysator for kvaliteten af projektet og besvarelsen af problemformuleringen.

# Problemfelt

Integreringen af IoT-enheder i virksomheder, er kommet for at blive. De teknologiske fremskridt kommer til at gå hurtigere ifm. udviklingen af IoT-produkter og set i forhold til dets potentiale, er det ikke unaturligt at virksomheder vælger at investere i IoT-systemer. I Danmark ser man derfor også en stigende interesse i at anvende IoT-systemer i erhvervslivet. Dog er der mange udfordringer forbundet med IoT-sikkerhed. Som beskrevet i indledningen, er det blevet estimeret at antallet af nye tilkoblet IoT-enheder vil ligge på mere end 20 mia. i 2020 på verdensplan. Ifølge Center for Cybersikkerhed vil der i de kommende år være et stigende antal af IoT-enheder i Danmark. I rapporten *Cybertrusler mod Danmark* fra 2019, beskriver de tendensen på følgende måde:

*"Der er flere risici forbundet med det stigende antal IoT-enheder, som kobles på internettet, og IoT-enheder anslås allerede nu at være blandt den type af enheder på internettet, der bliver udsat for flest cyberangreb"*
(Center for Cybersikkerhed, 2019; 16).

Her kan det konstateres at der er et stigende sikkerhedsmæssigt problem forbundet med IoT-enheder. Alt afhængigt af hvilken virksomhed det drejer sig om, findes der forskellige udfordringer ved IoT. Det medfører at mange hackere ikke kan modstå fristelsen, hvorved skaden er sket. Derfor har flere og flere virksomheder i stigende grad brug for vejledning til at kunne gennemskue de sårbarheder, der er ved brugen af IoT-enheder i erhvervsdrivende henseende. Men er disse udfordringer specifikt forbundet med IoT-systemer, eller er det de samme risici som gør sig gældende for generel IT-sikkerhed? Dette forsøger vi i denne undersøgelse at finde svaret på.

## Problemformulering

*Hvilke unikke sikkerhedsmæssige udfordringer skaber IoT-systemer og hvordan kan virksomheder forøge sikkerheden forbundet med disse systemer?*

### Arbejdsspørgsmål

*Hvor differentierer IoT-sikkerhed sig fra IT-sikkerhed?*
*Er der behov for specifikke retningslinjer for IoT-sikkerhed?*
*Hvordan er det nuværende trusselsbillede vedrørende IoT?*

# Afgrænsning

Vi har valgt at fokusere på IoT-miljøer i erhvervslivet og de dertil hørende sikkerhedsproblemer. Metodisk har vi valgt at begrænse os til litteraturstudie og kvalitative interview. I denne rapport undersøger vi ikke hvor stort et problem IoT-sikkerhed er for virksomheder, men nærmere hvorfor det er et problem og hvordan det opstår, samt hvilke konsekvenser det har for virksomhederne. Ved at fokusere på de unikke sikkerhedsmæssige udfordringer ved IoT, afgrænser vi os samtidig fra at beskrive sikkerhedsmæssige udfordringer ved generel IT-sikkerhed. Årsagen til at vi ikke har valgt at identificere enkelte virksomhedstyper og deres tilhørende IoT-problemer, er fordi formålet med rapporten er at give en generel vurdering af trusselsbilledet og sikkerhedstiltag, der vedrører IoT-miljøer i organisationer.

# Metode

Vores metodiske tilgang til projektet bunder i et litteraturstudie, hvor vi systematisk har samlet empiri fra tidligere studier, bøger samt videnskabelige artikler fra internettet. Empirien har dannet grobunden for vores videre arbejde med projektet og har skabt fundamentet for vores semistrukturerede interviews.

## Litteraturstudie

I projektet er litteraturstudiet benyttet som den primære metodisk tilgang til indsamling af empiri. Litteraturstudiet danner grundlaget for undersøgelsen og analysen af selve problemet (Eriksen, 2016). Vi har benyttet den tilgængelige litteratur, til at identificere de vigtigste termer, der relaterer sig til vores problemfelt. Det har vi gjort ved at indsamle eksisterende viden og teori, som har haft betydning for vores problemfelt. Metoden har givet os den tilstrækkelige baggrundsviden, som har været med til at forme udviklingen i projektet. Vi har forholdt os kritisk til den indsamlede empiri, samt diskuteret de mest centrale teorier og begreber. Vi har været vurderet validiteten af den litteratur, som er indgået i projektet. Det har hjulpet os med at skabe et stærkere grundlag for resten af opgaven. Da

begrebsfeltet inden for IoT er bredt og ændrer sig konstant, har litteraturstudiet også været en metodisk tilgang, der har gjort det muligt for os at differentiere i begreberne.

## Det semistrukturerede interview

Dette afsnit har til formål at introducere det semistruktureret interview og dets fordele og ulemper. Afsnittet vil også kort introducere centrale metodiske begreber, som er relevant for vores undersøgelse.

Der findes en bred vifte af forskellige metoder til at indsamle empiri. Hver metode har sine fordele og ulemper og netop derfor er det vigtigt at finde den metode, der matcher problemfeltet bedst. For at komme nærmere på en bevarelse af vores problemfelt, har vi valgt at foretage et semistruktureret interview med to eksperter inden for IoT-sikkerhed. Eftersom vi ønskede en større indsigt i genstandsfeltet, var en kvalitativ metodisk tilgang oplagt som valg. Ved hjælp af det semistrukturerede interview kan vi få informanternes erfaring og viden, som efterfølgende bruges som empiriske materiale. Når en eller flere metoder udvælges til en videnskabelig undersøgelse, er det vigtigt at tage højde for reliabilitet og validitet. Førstnævnte vedrører generaliserbarheden af undersøgelsen, det vil sige hvorvidt undersøgelsen kan gentages og give de samme resultater igen (Bryman, 2016; 157). Validitet berører gyldigheden af forholdene mellem problemstilling, de indsamlede data, samt konklusionen (Bryman, 2016; 158-159). Nærmere beskrevet henviser validitet til spørgsmål som:

”*Undersøger metoden det som der er hensigten?”* og *”reflekterer vores observationer i virkeligheden de fænomener der ligger i vores interesse”*

(Kvale, 1996; 238).

Validitet er således et begreb der kan hjælpe forskeren eller den studerende til en kritisk vurdering af egen undersøgelse, f.eks. ved at se nærmere på repræsentativiteten, søge efter negativ evidens, finde modsættende forklaringer eller gentage samme konklusion flere gange i andre miljøer (Kvale, 1996; 242). Reliabilitet og validitet er helt centrale begreber, som er nødvendige for at forbedre repræsentativiteten af vores undersøgelse. For at understøtte validiteten i undersøgelsen, har vi gennem vores litteraturstudie, prøvet at finde evidens som kan be- eller afkræfte informanternes udsagn. Vi har også haft stort fokus på om spørgsmålene, som vi udarbejdede, kunne bidrage til at besvare vores problemformulering. For at understøtte reliabiliteten har vi som tidligere nævn fokuseret på hvilke spørgsmål informanterne er blevet stillet. Det har været af stor betydning, da det semistrukturerede interview har været en essentiel del af vores metodiske tilgang.

## Fordele og ulemper ved det semistrukturerede interview

En fordel ved det semistrukturerede interview er, at der lægges stor vægt på informantens holdning og perspektiv. En ulempe kan være at informanten ikke har et tilhørsforhold til intervieweren og derfor kan det risikeres at informanten bevidst undlader visse informationer, eller at informantens udsagn er usande (Bryman, 2016; 466). Vedrørende transskribering har intersubjektiv reliabilitet også en central rolle. Begrebet henviser til at to personer som transskriberer samme lydfil ikke nødvendigvis har produceret to identiske dokumenter (Kvale, 1996; 236). Derfor kritiseres kvalitativ forskning også oftest på grund af manglende objektivitet. Videnskabeligt data skal være intersubjektivt reproducerbart og fænomener, der er observeret gentagne gange af forskellige observatører, skal give identisk data (Kvale, 1996; 64-64).

## Informanter

### Klaus Pedersen

Klaus Pedersen er Senior Security Architect hos Alexandra Instituttet. Klaus primære opgaver er at være med til at bringe teoretisk viden om bl.a. IoT-sikkerhed, IT-sikkerhedskultur og meget andet ud til danske virksomheder i en form, de kan forstå, og således bidrage til at nedbringe IT-sikkerhedsmæssige risici og understøtte en fortsat vækst i erhvervslivet.

### Alexandre Alapetite

Alexandre Alapetite er IT-ingeniør og er ansat som Senior Cyber-Physical Specialist på Alexandra Instituttet. Alexandre er ansvarlig for *Nordic IoT Centre,* som er et joint venture projekt mellem Force Technology og Alexandra Instituttet.

### Mikkel Brøndum

Mikkel Brøndum's jobtitel er *Certified Ethical Hacker* hos CGI. Brøndum er White Hat Hacker, hvilket betyder at han kender til hackeres metoder og værktøjer, men bruger disse til at rådgive virksomheder om IT-sikkerhed. CGI er en global IT-virksomhed, som primært levere konsulentydelser. Interviewet med Brøndum blev foretaget telefonisk.

### Valg af informanter

Vores informanter er udvalgt efter et ønske om at forstå sikkerhedsperspektivet omhandlende IoT fra flere vinkler. Vi ønskede at interviewe en ekspert indenfor IoT-sikkerhed for at få en større forståelse af vores genstandsfelt. Det førte til vores interview med Klaus Pedersen og Alexandre Alapetite. Det hjalp os med at forstå kompleksiteten, vedrørende IoT-sikkerhed ,og gav os samtidig et indblik i hvordan de rådgiver virksomheder, som ønsker at styrke deres sikkerhed indenfor IoT. Herefter kontaktede vi Mikkel Brøndum for at få et indblik i hvilke sårbarheder hackere udnytter, for at tiltvinge sig adgang til et IoT-system.

Ved udarbejdelsen og udførelsen af disse interview var vi klar over at det kan skabe bias at informanterne i begge interviews arbejder for konsulenthuse. Denne bias kan medføre at informanterne kan have en interesse i at få udfordringerne, vedrørende IoT-sikkerhed, til at fremstå større, for at fremme deres arbejdsområde. Vi har derfor i udarbejdelsen af vores interviewguide haft fokus på, hvilke sårbarheder der er ved IoT-systemer og ikke hvor stor truslen er. Dette har vi gjort for at formindske den eventuelle bias, der kunne forekomme i vores interviews.

Det sidste interview der blev foretaget med Mikkel Brøndum foregik telefonisk. Det har dog ikke haft betydning for kvaliteten af interviewet, da vi ikke skal analysere på informantens kropssprog og adfærd men derimod kun bruge informantens ekspertise indenfor genstandsfeltet.

## Sekundære kvantitative data

Vi har valgt ikke at udarbejde spørgeskema eller anden kvantitativ data. Det har vi valgt da der allerede findes spørgeskemaundersøgelser på området som har langt flere respondenter og dermed et langt større datasæt end vi ville være i stand til indsamle indenfor vores givne tidsramme. Vi har i dette projekt benyttes os af en sekundær kvantitativ undersøgelse, udarbejdet af Trend Micro, der er en virksomhed, som specialiserer sig i IT- og datasikkerhed. Denne undersøgelse er foretaget på 1150 IT-sikkerhedsansvarlige personer i virksomheder fra USA, England, Frankrig, Tyskland og Japan (Trend Micro, 2018; 2). Denne undersøgelse har vi benyttet for at få en forståelse af de globale organisatoriske udfordringer forbundet med implementeringen af IoT-enheder.

# De tre Hum-Tek dimensioner

I dette afsnit vil vi beskrive hvordan vi vil inddrage *STS, TSA* og *D&K* i bachelorprojektet. De tre dimensioner danner fundamentet for den humanistiske-teknologiske bacheloruddannelse på Roskilde Universitet.

## Subjektivitet, Teknologi & Samfund

I dimensionen *Subjektivitet, teknologi & samfund* arbejder vi med at handle aktivt i forhold til teknologien i vores samfund (Sommer, 2016). STS er grundlæggende en subjektivt orienteret tilgang til forståelse af teknologi, hverdagslivet og samfundsudviklingen og skal forstås som et konstitutionsforhold, hvilket vil sige at de 3 begreber i STS er betinget af hinanden. Vi vil derfor i denne dimension undersøge og diskutere IoT-sikkerheden ift. IoT-systemer, organisationer som anvender IoT og om der skal lave fælles retningslinjer for hvordan IoT-sikkerheden skal opretholdes.

## Teknologiske Systemer & Artefakter

I dimensionen *Teknologiske systemer & artefakter* vil vi undersøge IoT-sikkerheds udbredelse, samt kigge på de mekanismer der gør sig gældende, når et IoT-system bliver kompromitteret af et udefrakommende angreb (Sommer, 2016). Vi vil kigge på de fordele og ulemper som denne teknologi har medført. Dette vil vi gøre ved at identificere og analysere IoT-sikkerhed som en teknologi og vurdere IoT-miljøer som et større teknologisk system.

## Design & Konstruktion

I dimensionen *Design & konstruktion* er det vigtigt at forholde sig til designudvikling.
I denne opgave anvendes dimensionen til at beskrive den designløsning, der er gældende i dette projekt. I denne dimension inddrager og undersøger vi designløsninger såsom retningslinjer indenfor IoT-sikkerhed, eller mangel på samme. Derudover har vi udarbejdet egne modeller i opgaven bl.a. for at visualisere trusselsbilledet ifm. IoT-systemer, samt beskrevet hvad et IoT-system indeholder.

# Internet of things

Begrebet *Internet of Things*, dækker over det teknologiske fremskridt, hvor fysiske enheder kommunikerer sammen via et netværk. Da internettet blev annonceret for offentligheden i starten af 1990'erne, var det et vendepunkt, der skabte nye teknologiske muligheder. I begyndelsen fokuserede man hovedsageligt på at anvende internettet ifm. forbrugerservice og forretning. Nye forretningsmodeller opstod indenfor en bred vifte af brancher og de virksomheder, der ikke ændrede deres forretningsmodel, fik svært ved at overleve. I 1999 blev betegnelsen IoT for første gang anvendt af Kevin Ashton, der er teknologisk pioner og stifter af begrebet *Internet of Things*. Begrebet opstod i forbindelse med hans arbejde inden for *Radiofrekvensidentifikation* (RFID). Ifølge Ashton er vores samfund, økonomi og overlevelse ikke afhængig af ideer og information, men af ting:

> *" Yet today's information technology is so dependent on data originated by people that our computers know more about ideas than things. If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost."*
>
> (RFID Journal, 2009)

Ifølge Ashton er problemet at vi mennesker har begrænset tid, nøjagtighed og opmærksomhed, hvilket med andre ord betyder at vi ikke er gode til, at opfange alt data om andre ting i denne verden. Hvis vi derimod styrker elektroniske enheders evne til at indsamle, observere og identificere data, i denne verden, kan vi hermed udvinde nyttig viden om vores omgivelser og miljø. På denne måde kan vi løse en bred vifte af problemer, samt observere, identificere og forstå vores omgivelser bedre.
Der sker løbende en rivende udvikling indenfor IoT og i dag er vi vidner til en ny tendens, hvor vi oplever at internettet i større grad har fået indflydelse på vores dagligdag. Anvendelsen af kommunikationsteknologier har haft stor betydning for udviklingen og implementeringen af IoT-enheder i hjemmet og på arbejdet. Disse intelligente enheder kan interagere og kommunikere med hinanden over samme netværk. Ved at være forbundet til ét pågældende netværk, kan man derved fjernstyre disse enheder alt efter eget behov. Hertil kan enhederne indsamle data ud fra ens rutiner og vaner. Markedet for IoT-løsninger er ekspanderet de sidste mange år både inden for forbrugerelektronik og erhvervslivet. Disse produkter, dækker over mange forskellige områder, såsom *smarthome*, *wearables*, *SmartCity*, *Industrial internet of things*, *connected car* m.m. (ibid).

# IoT-sikkerhed

Alle disse enheder, som nu er forbundet til internettet, skaber også en øget sårbarhed for angreb, da man ikke længere har fysisk kontrol over produktet. Hackere kan fra den anden ende af verden fremtvinge sig adgang til enhederne, stjæle personfølsomme data eller noget helt tredje (Bilag 4; 5). Det er derfor vigtigt at virksomheder tænker datasikkerhed ind i alle aspekter af implementeringen af IoT-forbundne enheder. Denne tendens kaldes for *Security by Design,* som i sin enkelthed går ud på at man tænker sikkerhed ind helt fra starten. Dette begreb vil blive beskrevet nærmere senere i rapporten.

*"IoT vil hjælpe os med at blive mere effektive, sundere og mere sikre. Samtidig kan vi blive mere paranoide og usikre." (Bilag 4; 8).*

Sådan beskrives mulighederne og udfordringerne ved IoT i Alexandra Instituttets E-bog om IoT og sikkerhed (ibid). Her bliver det nævnt at IoT kan gøre brugere mere paranoide, hvilket kan skyldes en større risiko for hacker-angreb. Usikkerheden kan forbindes med den øgede kompleksitet i IT-infrastrukturen, som IoT-systemer medfører.


*Figur 1 - IT- og IoT-sikkerhed (bilag 4; 5)*

IoT-sikkerhed skal forstås som et delelement til generel IT-sikkerhed. Når man skal sikre IoT-enheder skal man tage alle de sikkerhedsforanstaltninger, som man gør ved almindelig IT-sikkerhed, men man skal samtidig forholde sig til nye udfordringer. Blandt disse udfordringer er et øget antal af

endepunkter som skal sikres, den øgede kompleksitet ved de mange forbundne enheder samt fysisk sikkerhed.

## Muligheder og udfordringer ved IoT

IoT er allerede en stor del af diverse brancher, som f.eks. sundhed og detail, samt mange statslige organisationer (Trend Micro, 2018; 2). IoT tilbyder nogle af de største innovative muligheder og redefinerer hvordan organisationer i industri og produktions sektorerne opererer, ved at gøre dem mere effektive og reducere omkostninger og udgifter. Som tidligere beskrevet forventes det at 20 milliarder IoT-enheder er tilsluttet i 2020. 67% af de tilsluttede IoT-enheder findes hovedsageligt i Kina, nord Amerika og det vestlige Europa (Gartner.com, 2017). Flere organisationer foretager ambitiøse tiltag for digital omstilling men det udsætter dem også for risikoen for angreb. En stor del af udfordringen bunder i at størstedelen af IoT-enheder er stærkt forankret i operationel teknologi (OT). Programmører som udvikler software til OT konsulterer sjældent med sikkerhedsansvarlige og opfylder dermed ikke security by design metoden. Det kan resultere i fatale konsekvenser for organisationen da det efterlader huller i sikkerhedsnettet, som f.eks. usikrede endepunkter. Hvis angriberen tvinger sig adgang til et endepunkt kan det bruges som en indgang til organisationens private netværk, hvilket kan give adgang til sensitiv data (Trend Micro, 2018; 2). Der tegner sig et billede af, at der simpelthen mangler kommunikation mellem sikkerhedsansvarlige og OT programmører og at dette fejlslagne samarbejde kan have fatale konsekvenser. Det er væsentligt at se nærmere på hvordan IoT-sikkerhed adskiller sig fra almindelig IT-sikkerhed. Alapetite forklarer i interviewet at IoT-sikkerhed kan ses som et *sub-asset* til almindelig IT-sikkerhed, hvor der ikke kun skal tages hensyn til de almindelige sikkerhedsaspekter men endnu flere sikkerhedsaspekter, f.eks. inden for fysisk sikkerhed. Pedersen tilføjer at sikkerheden indenfor IoT området er ret lav, fordi det historisk er set, at når en ny platform tages i brug, så glemmes tidligere oplevelser og erfaringer og der startes fra nul. En anden pointe er også at det først er når det er gået galt, at interessen for IT-sikkerhed vises (Bilag 1; 3).

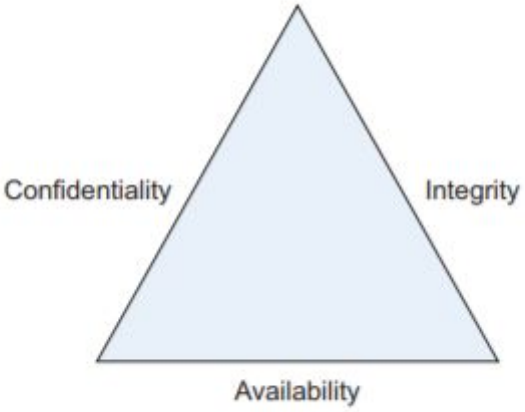
# Security by design

Security by design er et begreb som benyttes i udviklingen af applikationer og IT-systemer. Begrebet betyder at man skal tænke sikkerhed ind fra starten i udvikling og implementeringen af et IT-system. Security by design bygger på tre begreber som vil blive uddybet i nedenståe

# C-I-A triaden

*Confidentiality, Integrity & Availability* også kendt som *C-I-A triaden*, er sikkerheds principper som danner et sikkerhedsfundament og vejleder i at tænke IT-sikkerhed ind i organisationer (Pfleeger. C, et al. , 2015; 9). De tre sikkerhedsmål betragtes som værende essentielle for virksomheders IT-sikkerhed og hjælper dem med at identificere trusler og sårbarheder.

Som nævnt i problemfeltet er det essentielt for virksomheder at inkorporere sikkerhed helt fra start af. Det betyder at softwareudviklere og IT arkitekter har brug for vejledning til at designe sikrer applikationer.




Figur 2 - CIA (Perla, E. Et al , 2011; 35)

## Confidentiality

Dette sikkerhedsmål indebærer at der træffes foranstaltningerne i organisationen, der forhindrer følsomme oplysninger i at nå de forkerte mennesker. Dertil skal oplysningerne dog stadig nå ud til den ønskede modtager (Perla, E. et al, 2011; 36). Det betyder at adgangen skal begrænses til autoriserede personer, som herved kan tilgå den pågældende data. Man vil som regel kategorisere dataen ift. dens type og mængde. Dog kan det stadig være svært at sikre Confidentiality. Man skal i organisation internt vurdere hvem der er berettigede til at få adgang til visse systemer, samt kigge på den mængde af data de må tilgå (ibid). Dertil er det også vigtigt at uddanne og træne de autoriserede personer og gøre dem bekendt med de risikofaktorer, som følger med ansvaret. Det er en nødvendighed, hvis dataene falder i utilsigtede hænder. Ved at uddanne personalet, der har adgang til de fortrolige data, kan man dermed undgå et sikkerhedsbrud. Det kan f.eks. indebære at optimere IT-sikkerheden ved at

lave passwords, der er besværligere at afkode, eller informere medarbejderne om *Social engineering* (Pfleeger. C, et al, 2015; 80). Dette er en metode, som bl.a. anvendes af hackere til at snyde ansatte til at få udleveret fortrolige informationer.

### Integrity

Dette sikkerhedsmål vedrører opretholdelse af dataens indhold, nøjagtighed og troværdighed. Det er vigtigt fordi dataen ikke må ændres i sin transit mellem afsender og modtager (Perla, E. et al, 2011; 38). Dermed bliver man nødt til at tage forbehold i virksomheden, for at sikre at data ikke kan infiltreres af uautoriserede personer. Det indebærer at man laver foranstaltninger, der vedrører brugeradgangskontrol, som skal forhindre at der bliver lavet fejlagtige ændringer eller utilsigtet sletning af data. Dertil skal der anvendes midler til at bemærke ændringer i dataene, hvilket kan være forårsagede af ikke-menneskelige handlinger, såsom et server crash. Det kan eksempelvis være logning af data i det pågældende IT-system.

### Availability

Tredje sikkerhedsmål appellerer til at man i virksomheden vedligeholder al form for hardware og software for derved at holde det tilgængeligt (Perla, E. et al, 2011; 41). Det er en nødvendighed at opdatere IT-systemer. Man skal som virksomhed være forberedt på de værst tænkelige scenarier. Virksomhederne skal sikkerhedskopiere al data, da det kan have alvorlige konsekvenser, hvis der opstår problematikker i forbindelse med infiltrering fra uvedkommende. Det kan gøres ved at opbevare sikkerhedskopier på isolerede geografiske område. Derudover kan sikkerhedsudstyr, i form af proxy servere eller firewalls være med til at beskytte virksomheden mod ondsindede handlinger via indbrud i netværk, samt DoS angreb (Perla, E. et al, 2011; 42).

# Internet of Things taksonomi

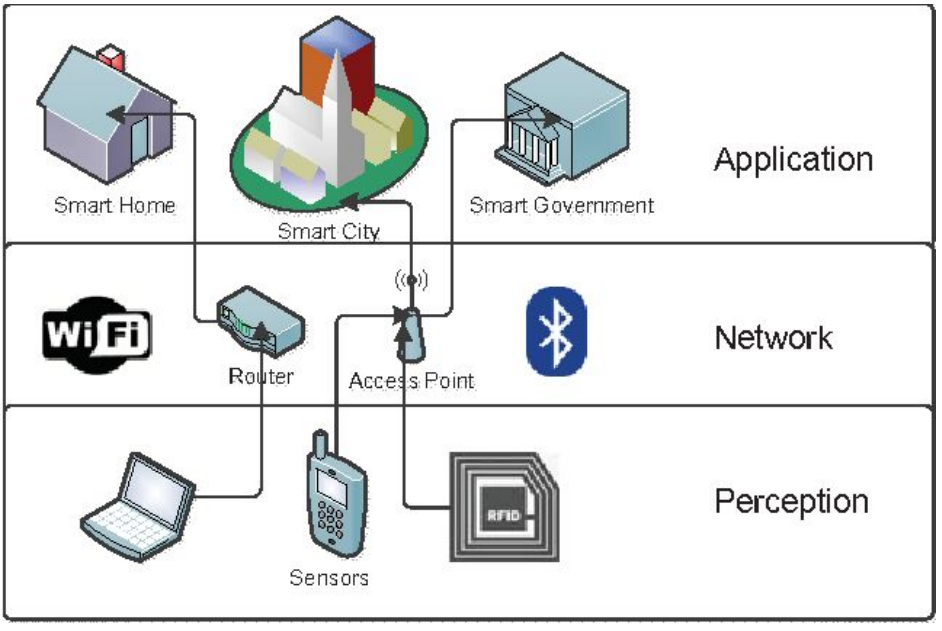
Følgende afsnit har til formål at beskrive Internet of Things taksonomi. Forståelsen af taksonomien er en nødvendighed for at kunne besvare problemfeltet og forstå de sikkerhedsaspekter IoT vedrører. Taksonomien kan beskrives ved de sikkerheds domæner og tilhørende sub-domæner som IoT består af. Alle elementer i dette afsnit har også til formål at give en generel forståelse af IoT og dets tilhørende kompleksitet.

| Sikkerheds domæner | Sub-domæner |
|---|---|
| Arkitektur | Logisk lag<br>Applikations lag<br>Netværks lag |
| Trusler | Fysiske angreb<br>kommunikationsangreb<br>Software angreb |
| Tillid | Pålidelighed<br>Tilgængelighed<br>Privatliv |
| Lovgivning | Politisk kontrol |

*Figur 3 – Egen udarbejdelse*

## Arkitektoniske domæne

Som beskrevet i *figur 3* består IoT af 3 operationelle lag og hvert lag har sin kernefunktion, hvilket også medfører at hvert lag har unikke sårbarheder. Derudover er der interdependens mellem hvert lag og dets funktioner, hvilket betyder at det logiske lags sårbarhed har betydning for de resterende lag og omvendt (Rizvi, et. Al, 2018; 164).




*Figur 4 - Visualisering af operationelle lag* (Semantic Scholar, 2015*)*

### Logisk lag

Det logiske lag, på engelsk kaldet perception layer, henter data til IoT-enheden og kan f.eks. indeholde sensorer som RFID. Disse sensorer kan indhente store datamængder. Derfor er det nødvendigt at laget er sikkert, så data ikke beskadiges eller manipuleres. Eftersom de fleste IoT-enheder er autonome, kan de let kompromitteres af angriberen. Der er dog forskellige sikkerhedselementer der kan tilføjes til laget for at undgå angreb som eksempelvis kryptering af data (Yang, Y. Et al, 2017; 1251).

### Applikationslag

Applikationslaget er det mest komplekse af de arkitektoniske lag, fordi der findes ekstremt mange forskellige IoT-produkter og producenter, som ikke følger en universel standard. Sikkerheds problematikken vedrører identitetsautentificering og dataadgang, da det kan være svært for virksomheden at administrere adgangstilladelser og godkendelser med alle de forskellige typer af applikationer og brugere på netværket. At sikrer data i applikations laget er en kæmpe udfordring fordi mængden af data er enorm og de mange endepunkter gør det sårbart. Til sidst skal det nævnes at der ligesom med andre typer af software tit findes sårbarheder i applikationslaget fordi udviklere ikke bruger standard kode indenfor deres applikationer (Swamy, S. Et. Al, 2017).

### Netværkslag

Netværkslaget i IoT vedrører overførslen af data og opererer på samme måde som et normalt netværk i TCP/IP. Derfor har netværkslaget i IoT de samme sikkerhedsproblemer som TCP/IP (Rizvi, et. Al, 2018; 164). Generelt for netværkslag er de klassiske typer af angreb: Virus angreb, DoS angreb, tyveri af intellektuel ejendom, Man-in-the-middle-angreb m.m. (ibid).

## Trusler

Når en angriber tvinger sig adgang til en IoT-enhed kan det gøres ved hjælp af forskellige typer af angreb. Eftersom angrebsfladen hos IoT-enheder både vedrører fysiske angreb og kommunikations angreb forøger det antallet af angrebstyper og øger derfor sårbarheden for angreb på IoT-enheder (Rizvi, et. Al, 2018; 165). Den øgede sårbarhed udnytter angribere ved hjælp af ondsindet kode og andre værktøjer. Da der findes en bred vifte af angreb berører dette afsnit kun de angreb, der er relevant for problemfeltet og den videre analyse.

## Kommunikations angreb

Denne form for angreb foregår over netværket og inkluderer angrebstyper som DoS, DDos, man-in-the-middle, SQL- og overflods angreb.

**DoS & DDoS**: Et DoS angreb sker når angriberen tvinger sig adgang til systemet/serveren og gør systemets funktioner ikke-brugbare for dets brugere. Et DDoS angreb foregår ved at angriberen tager kontrol over en større mængde computere/enheder (bots) og bruger dem til en overflod af forespørgsler, der resultere i at serveren bryder sammen og ikke er funktionel (ibid).

**Netværks injektion:** Angrebet kan opstå på alle enheder eller domæner, som anvender SQL databaser. Angriberen indfører ondsindet kode i databasen, hvorefter angriberen kan indhente, ændre eller slette informationer fra databasen. Eftersom IoT-enheder ofte gemmer informationer i flere forskellige databaser kan det risikeres, at angriberen får adgang til flere databaser gennem IoT-enheden og kan dermed gøre endnu større skade (ibid).

## Fysiske angreb

Disse angreb begrænser sig til fysiske angreb på netværket f.eks. gennem et kabel eller en trådløs forbindelse. Formålet med angrebet vil ofte være at beskadige IoT-enheden og derved blokere, optage eller transmittere beskeder mellem én eller flere IoT-enheder.

**Omvendt konstruktion:**
Angriberen bryder enheden ned i en række af trin for herefter at finde den fysiske enheds sårbarhed. Hvis sårbarheden bliver fundet kan alle enheder på det specifikke netværk angribes med samme metode (ibid). Et eksempel på sådan et angreb vil blive beskrevet senere i rapporten i det analyserende afsnit.

**Jamming:**
En ”jammer” er en enhed, der kommer i forskellige størrelser afhængigt af, hvilket signal der skal blokeres. Lavpraktisk fungerer det ved at blokere for et specifikt signal, f.eks. mobilsignaler, GPS signaler, radio signaler osv. På den måde kan enheden ikke modtage signalet og dens primære funktion ophører. Jamming bliver både brugt af hackere og imod dem, f.eks. bruger militære tjenester jammere til at blokere fjendens signaler.

**Manipulation af IoT-enheden:**
IoT-enheden bliver manipuleret allerede i udviklingsfasen eller i forsendelsesfasen. Angriberen manipulerer enheden, så enheden senere vil være tilgængelig for angriberen.

### Software angreb

**Cross site scripting (XSS):**
Denne form for angreb bruger også indskud af ondsindet kode. Angriberen omdirigere offeret til et andet websted og kan tvinge offeret til f.eks. at deltage i DDoS angreb eller stjæle sessioner. Ligesom med SQL-injektioner er datavalidering en nødvendighed for at undgå XSS angreb (Rizvi, et. Al, 2018; 166).

**Udnyttelse af fejlkonfiguration:**
Applikationer brugt af IoT-enheder kræver flere forskellige konfigurationer af systemer og komponenter for at operere korrekt. Hver af disse komponenter kræver også en ordentlig sikkerhedskonfiguration og er denne ikke fyldestgørende kan det udnyttes af angribere. Alt fra server og databaser til operativsystemer, kræver ordentlig konfigurationer for et sikkert IoT-miljø (ibid).

Som beskrevet i ovenstående afsnit har IoT-enheder en enorm angrebsflade og derfor er det ekstremt vigtigt at virksomheder fra start af vurderer risikoen vedrørende implementering af IoT-enheder. Senere i rapporten vil vi vurdere hvilke angrebstyper der er mest udbredt, samt hvilke konsekvenser det kan have for virksomheder.

## Tillid i IoT

I forbindelse med IoT kan tillid være svært at definere og må være subjektivt for den enkelte virksomhed. Det er ikke mange virksomheder, der kender til deres lag af sikkerhed i IoT-enheder og hvis enheden udføre sit formål, ser virksomheden ingen grund til bekymring. Prisen på en IoT-enhed er ofte en indikator for hvor sikker enheden er og virksomheder med et stramt budget har tendens til at nedprioritere sikkerhed i forhold til pris. Det resulterer i et usikkert IoT-miljø og kan have fatale konsekvenser for virksomheden og dens fremtidige forretninger (ibid). Tillidsbegrebet kan brydes ned i tre sub-domæner som vist i *figur 3*.

**Pålidelighed:**
At sikrer den data der transmitteres mellem IoT-enheder må være et grundlæggende ønske for alle virksomheder. Set i relation til den mængde af data der tit optræder i IoT-miljøer må sikkerheds principperne *Confidentiality, availibility, integrity* være et vigtigt aspekt i forhold til pålideligheden af et givent IoT-miljø.

**Tilgængelighed:**
IoT-enheder skal være tilgængelige for slutbrugeren for at opgaver kan udføres. Nogle IoT-enheder kan have funktioner, som lav strømstyring, slukket eller altid tændt og det kan være en fordel at afkoble enheden fra netværket i nogle tilfælde (Homeland Security, 2016; 12).

**Privatliv:**
Domænet optræder mest i det private forbruger aspekt men det kan også ske at en virksomheds IoT-miljø videresender informationer til tredjepart selskaber. Det kan være fortrolige virksomhedsoplysninger, som konkurrenter kan udnytter til deres fordel.

# Lovgivning

Lovgivning er et vigtigt aspekt i forhold til sikkerhed fordi det kan medføre standardisering indenfor IoT-sikkerhed. Under lovgivning kan virksomheder bedre organisere deres sikkerhed og forbedre den. Virksomhederne kan også selv vælge at lave intern lovgivning for at forbedre deres sikkerhedsrammer (Rizvi, et. Al, 2018; 166).

**Intern kontrol i virksomheden:**
Virksomheder skal gøre deres medarbejdere opmærksomme på hvilken skade deres brugernavn og password kan have på virksomheden, hvis det misbruges. Virksomheder kan også bruge en håndbog som guide til, hvordan medarbejderne kan være mere sikkerhedsbevidste i deres arbejde.

# GDPR

*Generel Data Protection Regulation*, eller GDPR, er en databeskyttelsesreform, der blev lanceret d. 25. maj 20018 (GDPR, UA). Formålet med GDPR er at danne et ensartede regelsæt i EU, der skal være med til at beskytte EU-borgernes rettigheder, når det vedrører personfølsomme oplysninger. (ibid). Det sker med henblik på at afværge, efterforske eller retsforfølge, strafbare handlinger der kan forekomme, når reglerne ikke bliver håndhævet af organisationer. Udrulningen af

Persondataforordningen (GDPR) har erstattet den tidligere Persondatalov. Det har medført at virksomheder måtte arbejde hårdt for at skulle sikre deres IT-systemer, samt leve op til de mange nye krav (Ibid). Især iværksætter firmaer har haft vanskeligheder med at gennemskue de mange krav som de er underlagt ved udruldnignen af GDPR. Det har skabt mange udfordringer for både de offentlige- og private virksomheder, hvilket har medført en frygt, da manglende efterlevelse af kravene kan ende ud i enorme bøder eller sanktioner (Ibid).

# En indeksering af IoT-trusselsbilledet

Som det første skridt i vores undersøgelse af de sikkerhedsmæssige trusler forbundet med IoT-enheder, var vi nødt til at undersøge om IoT-enheder overhovedet er forbundet med en øget sikkerhedsrisiko. Det kræver dog ikke meget dybdegående undersøgelse for at slå fast at, der er noget om snakken. I Center for Cybersikkerheds (CFCS) årlige trusselsvurdering over cybertruslen mod Danmark bliver truslen slået fast allerede i hovedvurderingen på de indledende sider:

*"Teknologiske udviklinger, såsom Internet of Things og kunstig intelligens, vil medføre nye muligheder til gavn for samfundet, men vil også åbne for en større angrebsflade for hackere. Der vil også være en øget risiko for, at cyberangreb kan medføre fysiske ødelæggelser, da enheder koblet til internettet i højere grad styrer fysiske systemer"*

(Center for Cybersikkerhed, 2019; 2)

Her nævnes det bl.a. at cyberangreb mod IoT-enheder kan føre til fysisk ødelæggelse, da IoT-enheder ofte styrer fysiske systemer. Derudover nævnes den øgede angrebsflade for hackere også som en udfordring for sikkerheden i IoT-systemer.
Der vil i det følgende afsnit blive gennemgået de største sikkerhedsmæssige udfordringer, som hovedsageligt er forbundet med IoT-systemer. Dette skal forstås som sikkerhedsmæssige udfordringer, hvor IoT-sikkerhed adskiller sig fra generel IT-sikkerhed.

## En forøget angrebsflade

Som nævnt i det ovenstående citat er en af de største udfordringer ved IoT-systemers sikkerhed, det øgede antal af endepunkter. Dette medfører at hackere har flere indgange til virksomheders IT-infrastruktur. Ifølge white hat hacker Mikkel Brøndum er det dog ikke det øgede antal IoT-enheder, i sig selv, som udgør en trussel, men det at angrebsfladen forøges:

*"[...] det her med at man øger angrebsfladen det behøver ikke altid ikke være en direkte risiko faktor eller direkte sårbarhed, men det er i hvert fald indirekte og kan gøre en mere sårbar, hvis man ikke er opmærksom på at hver gang man tilføjer en enhed til netværket, så øger man angrebsfladen."*

(Bilag 2; 3)

Ifølge Brøndum består problemet altså i, at man har flere endepunkter at holde styr på. Kapaciteten af enheder der skal sikres, er derved større og der er større risiko for sikkerhedsbrud. Den øgede angrebsflade kan hackere blandt andet benytte til at skabe botnets, der kan bruges i DDoS angreb som beskrevet tidligere i rapporten.
Et andet og meget lavpraktisk punkt, som relaterer sig til det forøgede antal af endepunkter, er det øgede antal af adgangskoder som det medfører. Selvom det at skabe sikre adgangskoder er meget banalt og muligvis det mest udbredte IT-sikkerhedsråd, så optræder usikre adgangskoder alligevel som nummer et på *Open Web Application Security Projects* (OWASP) liste over de 10 største sikkerhedsmæssige udfordringer vedrørende IoT (Bilag 3; 1). OWASP beskriver altså svage og hardcoded adgangskoder, som den største trussel for sikkerheden i IoT-systemer. Brøndum mener at installationen af enhederne har stor betydning i denne sammenhæng, da installatørerne oftest ikke har en stor viden om IT-sikkerhed:

*"De ændrer jo ikke passwordet eller i hvert fald ikke så det lever op til organisationens politik, som de formentlig heller ikke har. Der bliver tingene bare smidt ind som det er. Der er helt vildt mange af disse produkter som har default/ user password, så er det dét de kommer til at stå med. Det er noget som er totalt godt for sådan en som mig, for tit så er kameraer og IoT enheder, som vi snakkede om tidligere, et foothold"*

(Bilag 2; 4)

Her benævner Brøndum bl.a. at installatører af IoT-systemer ofte ikke ændre adgangskoden ved opsætningen af de enkelte enheder. Det beskriver han som et foothold, altså et startpunkt for hackere til at komme længere ind i virksomhedens IT-infrastruktur.

# Fysisk sikkerhed

En anden sårbarhed, som er kendetegnende for IoT-systemer, er den fysiske sikkerhed. Som beskrevet i CFCS trusselsvurdering i det indledende afsnit, kan angreb på IoT-systemer i højere grad fører til fysisk ødelæggelse, da IoT-enheder ofte benyttes til at styre fysiske systemer.
Alexandre Alapetite fra Alexandra Instituttet beskriver dette som en sårbarhed, der for det meste kun gør sig gældende ved IoT-systemer:

*"[...] hvor man selvfølgelig skal tage hensyn til de almindelige IT-sikkerhedsaspekter, de er der stort set alle sammen, men det er ikke nok. Man skal også tage hensyn til fysisk sikkerhed og det at folk kan få fysisk adgang til IoT, er noget som gør det svært."*

(Bilag 1; 2)

Det er altså en stor udfordring at sikre et IoT-system, hvis hackere kan få fysisk adgang til IoT-enhederne. Enheder, der er installeret i de omkringliggende omgivelser af en organisation, og som kommunikerer med organisationens intranet (eksempelvis sikkerhedskameraer, sensorer m.m.), er typisk fysisk ubeskyttet. Hackere kan på denne måde prøve at hente sikkerhedsnøgler fra enhederne til at komme videre ind i organisationens IT-infrastruktur, eller om-programmere enheden til at understøtte et nyt formål (Youm, 2017; 4). Fysisk sikkerhed er også repræsenteret på OWASP liste på en 10. plads, hvor de beskriver sårbarheden på følgende måde:

*"Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device."*

(Bilag 3; 1)

At fysisk sikkerhed ikke er højere på listen, skyldes sandsynligvis at det er meget tidskrævende for en hacker at udnytte denne sårbarhed, da de skal have fysisk adgang til enheden. Selvom sandsynligheden for denne form for angreb er mindre, er det dog en sårbarhed, som forekommer i mange IoT-systemer. Den fysiske sikkerhed relaterer sig samtidig ikke kun til den fysiske adgang til enhederne, men også til selve det hardware som enheden består af, hvilket gør denne sårbarhed til en af hovedårsagerne til mange andre sikkerhedsmæssige udfordringer.

## Mangel på sikre opdateringsmuligheder

Da mange IoT-enheder er små sensorer, som fungerer autonomt uden menneskelig interaktion, er mange af disse enheder ikke designet til at kunne blive opdateret. Dette beskriver CFCS som en sikkerhedsmæssig risiko forbundet med mange IoT-enheder:

*"Derudover er mange IoT-enheder ikke designet til at kunne modtage sikkerhedsopdateringer. Det betyder, at de sårbarheder, der bliver opdaget i produktets levetid, ikke kan rettes og derfor kan udnyttes af hackere, så længe produktet er i brug. Det er især et problem for IoT-enheder, der er designet til at kunne fungere i flere år uden menneskelig indblanding."*
(Center for Cybersikkerhed, 2019; 16)

Dette kan skyldes at mange IoT-enheder, er designet med en specifik funktion. Som tidligere nævnt har mange af disse enheder begrænsede computationelle færdigheder, hvilket gør at netværksfunktionen ,som gør dem i stand til at kommunikere med hinanden, er sekundær (ibid). Det er dog ikke kun manglen på sikkerhedsopdateringer, som kan være et problem. OWASP beskriver i deres top-10 også hvordan usikre opdateringsmuligheder kan skabe et sikkerhedsbrist. Dette kan blandt andet være manglende valideringsmuligheder eller manglende kryptering af signaler (Bilag 3; 1). Brøndum mener at dette problems ophav skal findes hos producenterne af IoT-enhederne:

*"Når man indkøber IoT enheder, så skal man allerede her have sikkerhed in mente. Her skal man selvfølgelig både stille krav til sikkerheden fra den distributør man køber det af, men også til producenten."*
(Bilag 2; 5)

Man skal ifølge Brøndum stille krav til producenten af enhederne, som f.eks. kvalitet af sensorer og release af patch. De begrænsede opdateringsmuligheder bliver også understøttet af Alapetite fra Alexandra Instituttet. Han mener at det er vigtigt at fremtidssikre enhederne til den dag der opstår et sikkerhedsproblem således, at man har en klar plan for hvordan dette problem kan løses. Alapetite mener at omkostningerne ved at forankre *security by design* i organisationers IoT-systemer, kan være en af hovedårsagerne til at der ikke er blevet gjort mere på området (Bilag 1; 2). Det skal understreges at det ikke er tilstrækkeligt kun at opdatere selve IoT-enheden, men at mobile applikationer og databaser som er tilknyttet enheden også skal opdateres (Mortensen, UÅ; 10). Desuden skal opdateringen af enheden ske gennem krypterede forbindelser, der bekendtgøre, hvem der må få adgang til at opdatere. På den måde sikres det at uvedkommende ikke kan udgive sig for at være en

opdateringsservice og få mulighed for at downloade skadelige kode til IoT-enheden, eller det netværk den er tilknyttet (ibid). Virksomhederne opdaterer typisk deres enheder pga. kendte sårbarheder, eller nye funktionaliteter. Det er derfor vigtigt at opdatere IoT-enheder, så snart nye opdateringer er tilgængelige, da hackere kan se i opdateringsversionen, hvilke sårbarheder der er blevet løst. Enheder der kører på gamle versioner af software, er derfor meget mere sårbare.

## Utilstrækkelig netværkssikkerhed

En anden sårbarhed for mange IoT-enheder, er utilstrækkelig netværkssikkerhed. Dette skyldes at mange IoT-enheder, i det logiske lag, er små komponenter som f.eks. sensorer eller chips med begrænsede computationelle færdigheder og begrænset lagerkapacitet (Alaba, F.A. Et. Al, 2017; 3). Det beskriver CFCS også i sin årlige cybertrusselsvurdering, hvor de beskriver udfordringen således:

*"IoT-enheder er ofte sårbare, fordi de bliver udviklet med et specifikt formål for øje, og de netværksfunktioner, som gør det muligt for enheden at kommunikere via internettet, er kun sekundære funktionaliteter. Derfor har enhederne ofte en utilstrækkelig netværkssikkerhed sammenlignet med traditionelt IT-udstyr, der er udviklet med henblik på at blive koblet på internettet."*
(Center for Cybersikkerhed, 2019; 16)

Denne sårbarhed optræder samtidig som nummer to på OWASP IoT-sikkerhedsliste (bilag 3; 1). Dette relaterer sig igen til den forøgede angrebsflade i det, at netværkssikkerheden kan kompromitteres fra flere endepunkter (Bilag 3; 1). Den utilstrækkelige netværkssikkerhed relaterer sig samtidigt også til den fysiske sikkerhed. Eksempelvis kan IoT-enheder jammes, så de ikke længere kan kommunikere med sin server (bilag 1; 12). Derudover kan denne angrebsmetode også bruges til at "lytte" til datatrafikken, som IoT-enheden udsender, hvilket understreger vigtigheden af at kryptere signaler mellem enheder.
En måde hvorpå organisationer forsøger at formindske denne sårbarhed, er ved at segmentere sit netværk. Brøndum beskriver dette som en af de vigtigste metoder for at øge netværkssikkerheden:

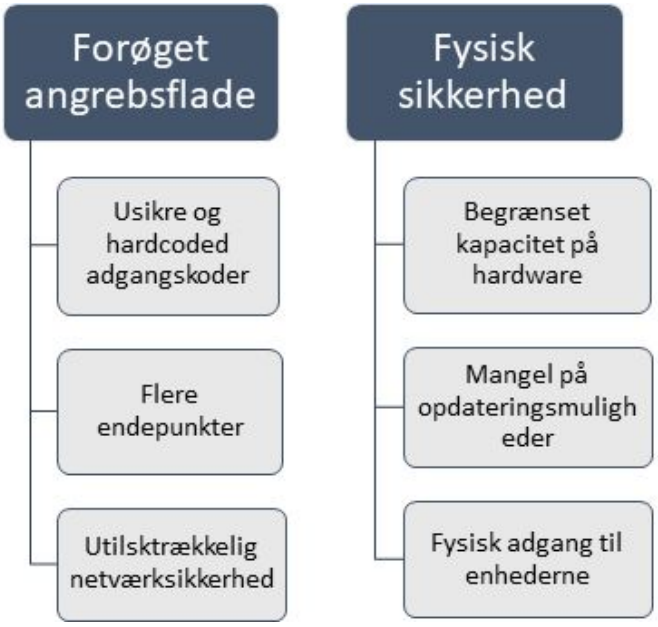
*"også skal man sørge for at segmenterer sit netværk, hvilket er det allervigtigste. Så det netværk, hvor der er IoT enheder forbundet, de er segmenteret i nogle segmenter."*
(Bilag 2; 8).

Ved at segmentere sit netværk kan virksomheder segmentere de dele af netværket, hvor IoT-enhederne er tilsluttet fra det administrative netværk og på denne måde øge sikkerheden på deres kritiske systemer og data. Brøndum benævner derudover også vigtigheden i at segregere sine netværk, hvilket

indebærer, at man ikke kan bruge de samme internetprotokoller på tværs af de segmenterede netværk (ibid). Et eksempel på dette vil blive benævnt senere i analysen.

## Model over unikke sårbarheder ved IoT-enheder

De unikke sikkerhedsproblemer, som relaterer sig til IoT-sikkerhed kan ud fra vores indsamlede og analyserede empiri koges ned til to hovedpunkter: En forøget angrebsflade og den fysiske sikkerhed.




*(Figur 5 - egen udarbejdelse)*

Under disse punkter er der opstillet underpunkter, som indikerer specifikke sårbarheder, der relaterer sig til en af hovedpunkterne. Modellen repræsenterer de unikke sårbarheder, som knytter sig til IoT-enheder. Det skal dog pointeres at opdelingen af sårbarhederne i denne model er meget firkantet opdelt og at underpunkterne relatere sig til hinanden. Eksempelvis er der et gensidigt tilhørsforhold mellem utilstrækkelig netværkssikkerhed og den begrænsede kapacitet i enhedernes hardware. Dette skyldes at enhedernes begrænsede computationelle færdigheder er en af årsagerne til at mange IoT-systemer har en utilstrækkelig netværkssikkerhed.

## Hvorfor angriber hackere IoT-systemer?

Der kan være mange forskellige årsager til angreb og det må antages at målet for angrebet vil være subjektivt i de fleste tilfælde. Hackerens incitament kan være politisk, økonomisk eller personligt. Er incitamentet politisk ses angrebene ofte i stor størrelse i form af DDoS angreb, hvor hackergrupper nedlægger større internetsider. Et eksempel på dette er beskrevet af Center for cybersikkerhed:

*"Et cyberangreb på en IoT-enhed kan påvirke enhedens funktion eller medføre en kompromittering af det netværk, som enheden er installeret i. Målet er ofte at installere malware på enheden, som gør det muligt for angriberen at fjernstyre den, så den kan udnyttes i andre cyberangreb. Kompromitterede IoT-enheder har typisk været brugt som led i overbelastningsangreb, hvor angriberen retter et meget stort antal enheders netværkstrafik mod en server og derved forsager et nedbrud."*

(Center for Cybersikkerhed, 2019; 16)

For at et angreb skal være succesfuldt har hackeren brug for 3 nødvendige elementer:


Figur 6 - egen udarbejdelse (Juul, 2018; 20)

Modsat kan virksomheden forsvare sig ved hjælp af 3 elementer:


Figur 7 - egen udarbejdelse (Juul, 2018; 20)

Det kan ofte være svært for virksomhederne at identificere formålet bag ved et angreb og hvis motivet er ukendt kan det være vanskeligt at underminere motivet. Der optræder tilfælde, hvor motivet bag

angrebet kan være angrebet i sig selv. Angriberen ønsker at bevise for sig selv, eller andre at han er i stand til at udføre et angreb. Det kan også være at systemet der angribes nærmest inviterer til angreb. Hvis det er et svagt system anses det som et nemt offer. At finde en præcis årsag til et angreb kan være komplekst, men hvis årsagen identificeres kan det give organisationen mulighed for at ændre deres sikkerhedsstrategi, for på den måde at undgå fremtidige angreb.

# Forbedring af IoT-enheders sikkerhedsniveau i organisationer

I forrige analyseafsnit undersøgte vi hvilke sikkerhedsmæssige trusler, der er unikke for IoT-enheder. Følgende afsnit forsøger at give et retvisende billede af hvad virksomheder generelt kan gøre for at hæve deres sikkerhedsniveau, samt finde løsninger på de trusler der er beskrevet i forrige analyseafsnit. De sikkerhedsråd som opstilles i dette analyseafsnit, er udarbejdet ud fra interview med informanter, samt tidligere studier der vedrøre IoT-sikkerhed.

For at finde ud af hvad en given virksomhed kan gøre for at øge sikkerheden i et IoT-miljø, er første del af processen at identificere hvor sårbarhederne eksisterer. Scenariet beskriver Brøndum ved at det generelt er svært for virksomhederne at identificere sårbarheden, da ekspertisen inden for feltet kan være en mangelvare i virksomheden (Bilag 2; 1). Et konkret eksempel på en sårbarhed kan også være en tidligere medarbejder, som er blevet afskediget. Hvis den ansatte har haft adgang til netværk og diverse systemer kan det være problematisk for virksomheden at identificere, hvad vedkommende er i stand til at forvolde af skade. Især sikkerheds principperne CIA, som er beskrevet tidligere i rapporten kan spille en stor rolle i et sådan tilfælde.

Ifølge Brøndum er den hyppigste efterspørgsel blandt offentlige og private organisationer en baseline, for hvilken situation de står i. Er deres sikkerhedslag optimale? Er systemerne opdateret og vedligeholdt korrekt? Flere virksomheder efterspørger også vejledning under opstartsfasen i implementeringen af nye IoT-systemer for at sikre at arkitekturen i systemet, er sikkert og holdbart (Bilag 2; 2). En helt central del af at forbedre sikkerheden i en virksomheds IoT-system, er at indkøbe IoT-enheder af ordenlig kvalitet som også kan patches. Brøndum beskriver problematikken i følgende citat;

*"...få startet med at købe noget der ikke er noget kinesisk bras, det er jo nok et af de vigtigste punkter. [...] Man skal også efterfølgende stille krav til hvordan man kan patche det. Man kan godt købe noget*

*der er rimeligt sikkert nu, men man kan også være sikker på at om et år er det usikkert. Hvis udstyret på en eller anden måde ikke kan skabe en patching proces eller manuel proces, så står man med et problem året efter."*

(Bilag 2; 4)

Ifølge citatet står det klart a,t der allerede skal tages hensyn til sikkerhed fra start og ifølge sikkerhedsdomænet *Tillid*, som beskrevet tidligere i rapporten, er det vigtigt at der er tillid til IoT-enheden og dets producent. Det er en generel problematik at virksomheder ofte vælger at købe billige IoT-enheder og de ofre på denne måde sikkerhed frem for pris (Rizvi, et. Al: 166). Dette kan være en stor beslutning for virksomheder at foretage og derfor kan det diskuteres hvorvidt denne beslutning alene skal foretages af virksomheden, eller om der skal være nogle statslige, eller internationale retningslinjer for IoT-sikkerheden, som de skal overholde. Dette vil blive diskuteret senere i rapporten. For at komme tillids problematikken til livs vil det være en fordel for virksomheden at bruge IoT-producenten som sparringspartner. Et videre samarbejde vil give mening for begge parter, da IoT-producenten vil fastholde sin kunde og virksomheden vil få den vejledning, der er behov for. Virksomheden vil f.eks. kunne undgå problemer med patching, da IoT-producenten løbende vil holde produkterne opdateret.
En anden problematik som tit opstår hos virksomheder, er den eksterne installation af IoT-enheder. De fleste nystartede virksomheder har ikke kompetencer, eller ressourcer til selv at installere IoT-enheder. Et tænkt eksempel kunne være en mindre markedsføringsvirksomhed, som føler at deres materielle aktiver har nået en så høj værdi, at der er behov for et overvågningssystem til deres domicil. I ledelsen vurderes budgettet og et overvågningssystem passende til budgettet indkøbes. Her opstår første brist i sikkerhedsniveauet. Det står klart at virksomheder må indkøbe systemer, der passer til deres budget men det er værd at overveje sin investering i overvågningssystemer. Dette understreger Brøndum også i følgende citat:

*"For eksempel sådan nogle som Dahua Hikvision er top 1 og 2 af de mest sælgende kamera producenter i Europa og de har den vildeste track record for sårbarheder og sårbarheder som man mener er placeret med vilje i firmwaren"*

(Bilag 2; 5)

Derfor må et klart sikkerhedsråd være at virksomheder, der bruger overvågningssystemer skal undersøge producenten nøje inden et givent produkt bliver købt. Et andet bud i relation til forrige må være at rådføre sig med sikkerhedseksperter, der ved hvilke producenter der er kendt for at have mange sårbarheder i deres produkter.

Problematikken vedrørende sårbarhederne i IoT-enhederne leder videre til det næste sikkerhedsbrist, som opstår i forlængelse af et overvågningssystem. For at konkretisere problemet vil det forrige tænkte eksempel uddybes. Lad os antage at den mindre markedsføringsvirksomhed indkøber et overvågningssystem udelukkende baseret på deres budget og derfor også på pris. Overvågningssystemet er kendt for sårbarheder, men det ved virksomheden ikke, da deres viden indenfor området ikke er tilstrækkeligt. En installatør fra producenten kommer og installerer systemet og her opstår næste sikkerhedsbrist. Brøndum beskriver problematikken således:

"*De er ikke uddannet i denne form for sikkerhed. Det er sikkert gode installatører og gode til at smække nogle kameraer op og trække kabler også gør de det. De ændrer jo ikke passwordet eller i hvert fald ikke så det lever op til organisationens politik, som de formentlig heller ikke har. Der bliver tingene bare smidt ind som det er.*"

(Bilag 2; 4)

Problematikken viser sig at være paradoksalt, da virksomhederne tit ønsker at forbedre deres sikkerhed i form af et overvågningssystem, men i stedet ender med en øget sårbarhed overfor angreb. Især virksomheder med immaterielle aktiver af høj værdi kan risikere at skade deres forretning voldsomt, hvis ikke de tager sikkerhedsvurderinger alvorligt.

## Segmentering af netværk

Det næste sikkerhedsråd som virksomheder bør benytte sig af, er segmentering af netværk. Hvis hackeren udnytter de sårbarheder, som ligger i IoT-systemet kan virksomhederne risikere at få kopieret patenter, forretningsstrategier eller andre intellektuelle ejendomme. Det mener Brøndum kan undgås ved segmentering af netværket;

*"Man segmenterer det væk fra sit administrative netværk og hvad man ellers har. Så hvis man taber en zone, så taber man ikke alle zoner og jeg ser rigtig tit nogle netværk der er struktureret sådan at hvis jeg kan overtage et kamera, der står ude på en parkeringsplads, så kan jeg infiltrere deres netværk og komme ind i deres interne mail og fileserver på det administrative netværk og det er jo ikke meningen."*

(Bilag 2; 6)

For at undgå manipulering af sine IoT-enheder mener Brøndum, at segmenteringen af netværket i sig selv ikke er nok, men at virksomhederne også skal segregere det. Brøndum uddyber med et eksempel

fra en kunde han har arbejdet tæt med. Virksomheden har et ekstremt stort netværk, som er segmenteret i små segmenter og ønsker at nogen segmenter skal have adgang til andre, men ikke omvendt. F.eks. skal *segment 1* kunne se et kamera i *segment 2,* men det skulle ikke være muligt at komme videre til *segment 3*, som er et kritiske punkt (Bilag 2; 7). Det kamera som kunne tilgås fra *segment 1* til *segment 2* havde en sårbarhed, der gjorde at Brøndum kunne overtage og bruge det som foothold. Det gav ham adgang til kameraet, hvorpå han kunne ligge en *SOCKS5 Proxy,* som er en internet protokol (Nordvpn.com, 2015). Denne internet protokol gjorde Brøndum i stand til at sende data gennem en proxy server, som generer en arbitrær IP adresse inden destinationen er nået og på den måde tvinge sig adgang til *segment 3* (ibid). På den måde var Brøndum i stand til at manipulere med netværket ved hjælp af en IoT-enhed, som havde en sårbarhed.
Brøndum argumenterer efterfølgende for at virksomheden faktisk havde en fin og velfungerende IT-arkitektur, men pga. af at netværket ikke var segregeret ordentligt, skabte det en sårbarhed;

*"Man kunne ikke gå fra segment 1 til segment 3, men fordi at der var en eller anden installatør, som havde sat et Flir kamera ind, men ikke patched det, så gjorde man det muligt for mig at komme ind i netværket. Så man skal segmentere, også skal man segregere, fordi hvis nu de også havde segregeret netværket, så kunne det være at der var nogle der tænkte om der var en årsag til at det her kamera kunne oprette en RDP-forbindelse til segment 3, for det var faktisk det jeg gjorde. Jeg kunne sidde og lave fjernskrivebord, altså RDP fra segment 1 til segment 3 over et kamera og det er der ingen grund til at dette kamera skal kunne etablere."*

(Bilag 2; 7)

*RDP* står for remote desktop control og gør brugeren i stand til at styre enheden. Brøndum uddyber at det kan være vigtigt at fjerne funktioner fra en enhed, for på den måde at undgå manipulering af netværk og derudover have en form for overvågning af sit netværk.

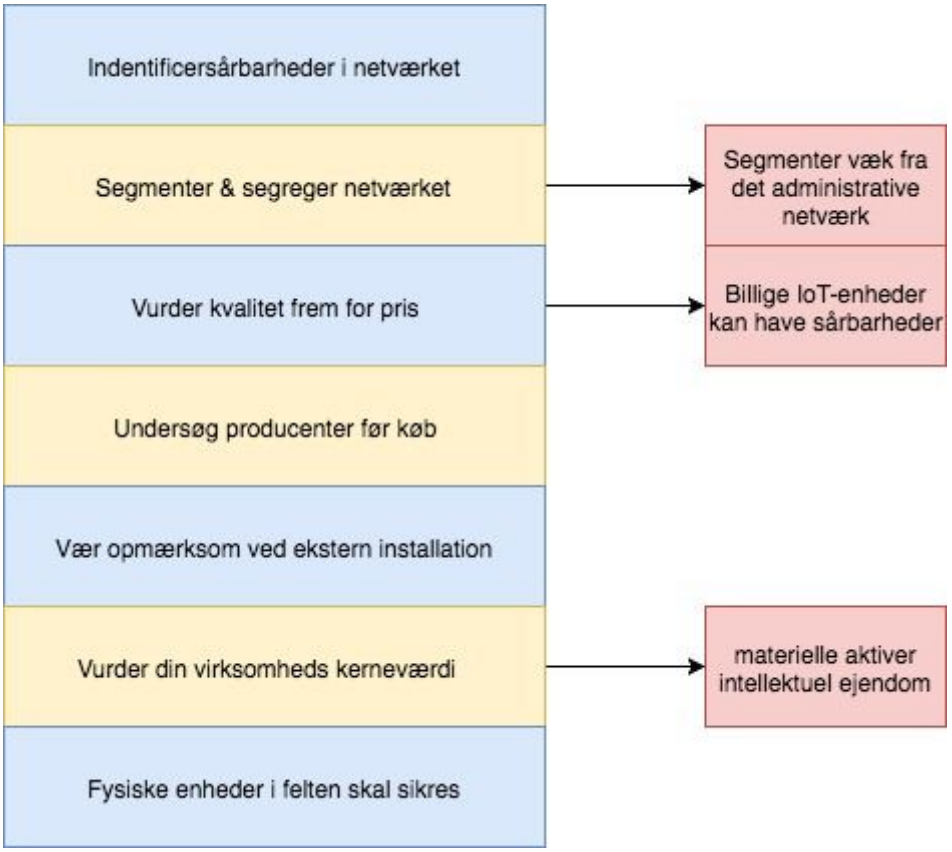
*"Det kan være at det skal kunne sende billeder over og ikke andet. Så det her med at segmentere og dele det op og det her med at segregere, så man ikke bare kan bruge alle protokoller på kryds og tværs. Så er det også noget med at når man har IoT enheder, så kan det også give rigtig meget mening at have en form for overvågning af ens netværk og beskyttelse af netværket."*

(Bilag 2; 7)

Brøndum argumenterer altså ligeledes for at det kan være effektivt at monitorer organisationers netværk for på den måde at identificere usædvanlig og uønsket kommunikation på netværket.

Dette er samtidigt en af de mest anvendte strategier blandt organisationer, for at sikre sine IoT-systemer mod angreb, hvorpå 56% af organisationer har størst fokus på dette (Trend Micro, 2018; 4).

I ovenstående afsnit er eksempler fra situationer som vores informant har oplevet. De forskellige situationer er basale eksempler på hvorfor sikkerhedsbrist opstår i forbindelse med IoT-enheder, men også hvordan de kan undgås. For at opsummere sikkerhedsforslagende fremstillet i ovenstående analyse vil nedenstående figur være vores bud på, hvad virksomheder kan gøre for at optimere deres sikkerhedsniveau vedrørende IoT-enheder.




Figur 8 - egen udarbejdelse

# IT-sikkerhed før og efter IoT - er der behov for nye retningslinjer?

Som belyst tidligere i rapporten har organisationer svært ved at overkomme de sikkerhedsmæssige udfordringer ved IoT-sikkerhed. I Trend Micros undersøgelse var det bl.a kun 27% af de adspurgte IT-ansvarlige, som ikke havde oplevet et angreb på deres IoT-systemer inden for det seneste år (Trend Micro, 2018; 4). Men skyldes dette en mangel på regler og standarder inden for IoT-sikkerhed, eller gskyldes det derimod at virksomheder ikke investerer nok tid og penge i sikkerheden?
Det kan være svært, hvis ikke umuligt, at komme med en endelig konklusion på dette spørgsmål. Sandheden er nok nærmere at sikkerheden varierer fra organisation til organisation og at der allerede findes krav og standardiseringer, som berør IoT-enheder. Spørgsmålet er derfor nærmere om der mangler krav som henvender sig specifikt til IoT-produkter. I den nye persondataforordning fra 2018 er der bl.a. sat krav til "*Data protection by design and default*" som Ico, Englands uafhængige myndighed for overholdelse af informations rettigheder, uddyber i deres guide til GDPR:

*"This concept is not new. Previously known as 'privacy by design', IT has have always been part of data protection law. The key change with the GDPR is that IT is now a legal requirement."*
(Ico, 2018; 175).

Begrebet *privacy by design* som er beskrevet tidligere i opgaven, er altså nu et juridisk krav til virksomheder, som skal implementere IT-systemer eller applikationer og er dermed også et krav til IoT-systemer. Til trods for disse nye regler er der dog meget, der tyder på at sikkerheden inden for IoT stadig ikke bliver prioriteret fra start. I Trend Micros rapport skriver de blandt andet:

*"Despite the clearly perceived risks, few organisations involve security teams in projects from the start."*
(Trend Micro, 2018; 3).

Dette mener Pedersen fra Alexandra Instituttet dog også gør sig gældende indenfor generel IT-sikkerhed:

"*Det er et problem også generelt med IT-sikkerheden er der det sædvanlige med at man først interessere sig for sikkerheden når noget går galt. Det er vi altid op imod.*"
(Bilag 1; 3).

Man kan i denne sammenhæng diskutere hvorvidt lovgivning og oplysning hjælper med at forankre *security by design* hos organisationer. Det gør sig dog også gældende ved generel IT-sikkerhed og er ikke et fænomen, der er unikt for IoT-sikkerhed. Som en kommentar til de manglende standarder inden for IoT-enheder svarede Brøndum følgende:

*"Nej, det tror jeg bestemt heller ikke på der er og der kan man sige at i hvert fald for offentlige og statslige organisationer, der synes jeg som minimum kravet er at der er nogen der har lagt hjernen bare lidt i blød også skrevet at de og de producenter skal man ikke købe af [...]"*
(Bilag 2; 9).

Brøndum argumenterer i denne sammenhæng, for at der skal stilles krav til producenterne af IoT-enhederne. Som tidligere nævnt, er der stor sikkerhedsmæssig forskel på IoT-enheder fra producent til producent. Brøndum uddyber denne problematik således:

*"[...] det er tit noget jeg undrer mig over i forhold til forbrugerstyrelsen, som jo går super meget op i at der ikke er alt muligt i vandhaner som man køber, men når det kommer til elektronik, så er der totalt frit slag."*
(Bilag 2: 5)

Man kan derfor argumentere for at der skal opstilles specifikke krav til producenterne af IoT-enheder. Som tidligere nævnt kan der være stor forskel på hardware-sikkerheden blandt IoT-enheder alt efter producenten. Brøndum argumenterer derfor for at forbrugerstyrelsen bør sætte krav til elektroniske enheder. Dette er man enige i hos Dansk Standard, Danmarks officielle standardiseringsorganisation, som anbefaler at forbrugerorganisationer skal være med til at påvirke internationale standarder, der er under udvikling så der i højere grad også bliver taget hensyn til forbrugere af IoT-enheder (Dansk Standard, UÅ; 19). I forbindelse med de manglende retningslinjer indenfor IoT-sikkerhed, er der også et behov for certifikater, så virksomheder kan bevise at de opfylder de gældende krav:

*"[...] vi går ind og undersøger hvilke compliance krav der er til IoT-sikkerheden og hvad virksomhederne skal gøre hvis de gerne vil have blåstemplet deres produkter, men det giver bare ikke*

*nogen mening, når der ikke er nogle krav."*
(Bilag 1; 15)

Her forklarer Pedersen at det kan være problematisk for producenter af IoT-enheder at bevise at deres IoT-sikkerhed er i orden, hvis ikke der er nogle specifikke krav de kan vise at de overholder. Pedersen henviser til medicinalindustrien, hvor man skal verificeres for at kunne sælge sit produkt i forskellige lande (ibid). Det mener Brøndum også er en god idé og henviser til USA, hvor man har lavet et forbud mod sikkerhedskameraer fra Dahua og Hikvision i statsejede bygninger, da der tidligere er opdaget sårbarheder i disse sikkerhedskameraer (Bilag 2; 9). Man kan i denne sammenhæng argumentere for at de overordnede krav til IT-sikkerhed også gør sig gældende for IoT-sikkerhed, bl.a. i forbindelse med ikrafttrædelsen af persondataforordningen. Dog kan man argumentere for at der skal laves specifikke hardware og software relaterede krav til producenterne af IoT-enheder, som skal overholdes for at produkterne skal kunne sælges i Danmark.

Som tidligere nævnt savner eksperter på området specifikke krav til virksomheders håndtering af IoT-sikkerhed. Der er findes i dag overordnede krav til IT-sikkerhed, som også vedrøre IoT-sikkerhed bl.a. GDPR og ISO27001. Det kan imidlertid være svært for virksomheder at gennemskue, hvordan disse krav relaterer sig til IoT-sikkerhed. I den forbindelse har flere forskellige organisationer udarbejdet vejledninger for håndtering af IoT-sikkerhed, heriblandt, Dansk Industri og Alexandra Instituttet. Selvom disse vejledninger kan hjælpe virksomheder med at håndtere IoT-sikkerhed kan man diskutere, hvorvidt statslige eller internationale retningslinjer vedrørende IoT-sikkerhed ville skabe et mere homogen forståelse på området. Dansk Standard har sågar udgivet en rapport kaldet *"Roadmap om standarder for Internet of Things (IoT)"* (Dansk Standard, UÅ), hvilket giver et billede af hvor komplicerede standardiseringerne inden for IoT er i dag. I rapporten bliver den fragmenterede udvikling af standarder beskrevet på følgende måde:

*"Samtidig er der virksomheder og private organisationer, der udvikler deres egne standarder, hvilket skaber dynamik, men samtidig kan skabe markedsfragmentering. Det gælder fx IEEE, IETF og OASIS (såkaldte konsortier). Det kan være en god ide at bygge videre på initiativer, som allerede findes på markedet. Men det bør gøres på en måde, så der skabes fælles internationale standarder, der understøtter fri konkurrence på markedet."*
(Dansk Standard, UÅ; 5).

Her bliver det beskrevet hvordan private organisationers standarder kan skabe markedsfragmenteringer. Det kan være problematisk, da det kan skabe en differentiering af IoT-sikkerhed fra marked til marked. Samtidigt kan det også skabe en differentiering af

IoT-sikkerheden fra land til land, hvilket kan føre til at lande, ved at lempe deres krav for IoT-sikkerhed, kan skabe en konkurrencefordel inden for et givent marked. Man kan dermed argumentere for, at der skal skabes fælles internationale standarder på området for at undgå segmentering, som kan skabe forvirring og kan være konkurrenceforvridende.

# Konklusion

Det står klart at virksomheder, der bruger IoT-enheder i deres netværk har en forøget angrebsflade. I analysen har vi forsøgt at komme til bunds i, hvordan virksomheder bedst kan sikre sig imod udefrakommende angreb. Vi kan konkludere, ud fra vores empiriske grundlag, at organisationer oplever problemer når de skal; [1] vurdere risiko for angreb på IoT-enheder, [2] Organisere og overvåge egne netværk, [3] segmentere og segregere IoT-netværk, [4] vurdere kvaliteten af IoT-enheder, [5] inkludere *Security by design* i implementering af IoT-systemer og [6] patche deres IoT-enheder.

Ovenstående er 6 eksempler på generelle problematikker, som organisationer kæmper med, når IoT-teknologi skal implementeres i deres forretning. Dette er samtidig også vores bud på sikkerhedsråd, som bør inkluderes i fremtidige internationale standarder for IoT-sikkerhed. Vi kan samtidig konkludere at de unikke sårbarheder ved IoT-systemer kan deles op i to hovedpunkter; en forøget angrebsflade og fysisk sikkerhed. Det kan også konkluderes at der er et behov for overordnede internationale standarder som er unikke for IoT, da det sikre fri konkurrence og er med til at reducere markedsfragmentering. Herunder unikke krav til producenter af IoT-enheder med henblik på at øge den fysiske sikkerhed. Det er også vigtigt at pointere at IoT-enheder er påvirket af et globalt marked. Derfor vil producenterne først på markedet med deres produkt og det betyder i nogle situationer at produkterne ikke er af den bedste kvalitet. Derudover kan det også konkluderes at sikkerhed er dyrt at forankre i IoT-enheder og derfor tit bliver nedprioriteret af producenten.

Til sidst kan det konkluderes at IoT-systemer skaber nye og unikke muligheder for organisationer. Dog medfører IoT-systemer også nye udfordringer i form af en øget kompleksitet i IT-infrastrukturen. Derfor skal organisationer, lovgivning og producenter følge hinanden i den fortsatte udvikling indenfor Internet of Things.

# Litteraturliste

**Bøger**

Bryman, Alan. "*Social Research Methods"*. Oxford University Press, 2016.

Kvale, Steinar. "*Interviews: an Introduction to Qualitative Research Interviewing"*. SAGE, 2008.

Perla, E., & Oldani, M. "*A Guide to Kernel Exploitation",* 36-47. 2011.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. *Security in Computing*, 5th Edition, 9-40. 2015

## Artikler

Alaba, F.A. Et. Al. "*Internet of things Security: A Survey*", University of Malaya, (2017). Internetadresse: https://www.researchgate.net/publication/315835782_Internet_of_things_Security_A_Survey - Lokaliseret d. 04.04.2019 (Internet)

Rizvi, et. Al, "*Securing the Internet of Things (IoT): A Security Taxonomy for IoT"* Pennsylvania State University, (2018), s. 163-168. Internetadresse: https://www.researchgate.net/publication/327478710_Securing_the_Internet_of_Things_IoT_A_Security_Taxonomy_for_IoT - Lokaliseret d. 19.05.2019 (Internet)

Swamy, S. Et. Al. "*Security threats in the application layer in IOT applications"* I-SMAC (IoT in Social, Mobile, Analytics and Cloud). Palladam, India: IEEE. (2017). Internetadresse: https://www.researchgate.net/publication/320252452_Security_threats_in_the_application_layer_in_IOT_applications - Lokaliseret d. 17.04.2019 (Internet)

Yang, Y. Et al. "*A Survey on Security and Privacy Issues in Internet-of-Things"* IEEE, Internet of Things Journal, (2017) s. 1250-1258. Internetadresse:

https://www.researchgate.net/publication/316173391_A_Survey_on_Security_and_Privacy_Issues_in_Internet-of-Things - Lokaliseret d. 25.04.2019 (Internet)

Youm, Heung Youl: *An Overview of Security and Privacy Issues for Internet of Things*. I: *IEICE*, (2017), s. 1-4. Internetadresse: https://www.researchgate.net/publication/309375790_Internet_of_Things_Security_and_Privacy - Lokaliseret d. 20-04.2019 (Internet)

## Rapporter

Center for Cybersikkerhed, "*Cybertruslen mod Danmark"*, 1. udgave, (2019). Internetadresse: https://fe-ddis.dk/cfcs/publikationer/Documents/Cybertruslen-mod-Danmark-2019.pdf - Lokaliseret d. 24.04.2019 (Internet)

Dansk Standard, *"Roadmap om standarder for Internet of Things (IoT)"*, Fonden Dansk Standard, UÅ. Internetadresse: https://www.ds.dk/~/media/DS/Files/Downloads/iot/Roadmap-for-standarder-om-IoT_januar2017.ashx?la=da - Lokaliseret d. 24.05.2019 (Internet)

Homeland Security, "*Strategic Principles for Securing the Internet of Things (IoT)*" U.S. Department of Homeland Security, (2016). Internetadresse: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf - Lokaliseret d. 10.05.2019 (Internet)

Mortensen, Henning, Dansk Industri, *vejledning: Sikkerhed i Internet of Things*, DI Digital, UÅ. - Internetadresse: https://digital.di.dk/SiteCollectionDocuments/Vejledninger/Sikkerhed%20i%20Internet%20of%20Things.pdf - Lokaliseret d. 24.05.2019 (Internet)

Trend Micro, *The IoT Revolution: Uncovering Opportunities, Challenges and the Scale of the Security Threat*, (2018). Internetadresse: https://documents.trendmicro.com/assets/rpt/rpt-IOT-report.pdf - Lokaliseret d. 08.05.2019 (Internet)

# Hjemmesider

*Basiskursus 3: Teknologiske systemer og artefakter I, 1. semester* - (2016). Udgivet af Roskilde Universitet. Internetadresse: https://study.ruc.dk/class/view/14418 - Lokaliseret d. 15.05.2019 (Internet)

*Benefits of using SOCKS5 Proxy* - (2015). Udgivet af Nordvpn. Internetadresse: https://nordvpn.com/da/blog/socks5-proxy/- Lokaliseret d. 18.04.2019 (Internet)

*Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* - (2017). Udgivet af Gartner Inc. Internetadresse: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 - Lokaliseret d. 28.04.2019 (Internet)

*Hvad er GDPR?* - (2019). Udgivet af GDPR. Internetadresse: https://gdpr.dk/ - Lokaliseret d. 22.05.2019 (Internet)

*Hvad er ISO27001?* - (2019) Udgivet af Digitaliseringsstyrelsen. Internetadresse: https://digst.dk/sikkerhed/iso27001/hvad-er-iso27001/ - Lokaliseret d. 24.05.2019 (Internet)

*Internetbrug og enheder 2015* - (2015). Udgivet af Mediernes udvikling. Internetadresse: https://mediernesudvikling.slks.dk/fileadmin/user_upload/dokumenter/medier/Mediernes_udvikling/2015/Internetbrug_og_enheder/Hovedresultater/Hovedresultater_Internetbrug_og_enheder_2015.pdf- lokaliseret d. 01.05.2019 (Internet)

Internet of things (IoT) security: Current status, challenges and prospective measures (2015). Udgivet af Semantic Scholar. Internetadresse: (https://www.semanticscholar.org/paper/Internet-of-things-(IoT)-security%3A-Current-status%2C-Mahmoud-Yousuf/add4396a95b96927dbef194b2657800312553e21/figure/0 - Lokaliseret d. 24.05.2019 (Internet)

*Sådan foretager man et litteraturstudie* - (2019). Udgivet af Eriksen, Thor. Internetadresse: https://www.scribbr.dk/struktur-i-din-afhandling/saadan-foretager-man-et-litteraturstudie/ - Lokaliseret d. 01/04.-2019

*That 'Internet of Things' Thing. Udgivet af RFID Journal* - (2009). Internetadresse: https://www.rfidjournal.com/articles/view?4986 - Lokaliseret d. 16.04.2019 (Internet)

## Slides fra forelæsninger

Sommer, F. M. (2016, September 13). *"introduktion til STS"* [pdf]. Lokaliseret på: https://moodle.ruc.dk/course/view.php?id=7559

Juul, C. N. (2018, oktober 2). *"Organisatorisk forandring og IT"*. Lokaliseret på: https://moodle.ruc.dk/course/view.php?id=10753

## Bilag

Se bilagene i vedhæftede dokumenter

Bilag 1: Transskribering af interview med Alexandra Instituttet

Bilag 2: Transskribering af interview med Mikkel Brøndum

Bilag 3: OWASP top 10 liste

Bilag 4: Alexandra Instituttet - Om IoT sikkerhed