AALBORG UNIVERSITET
STUDENTERRAPPORT

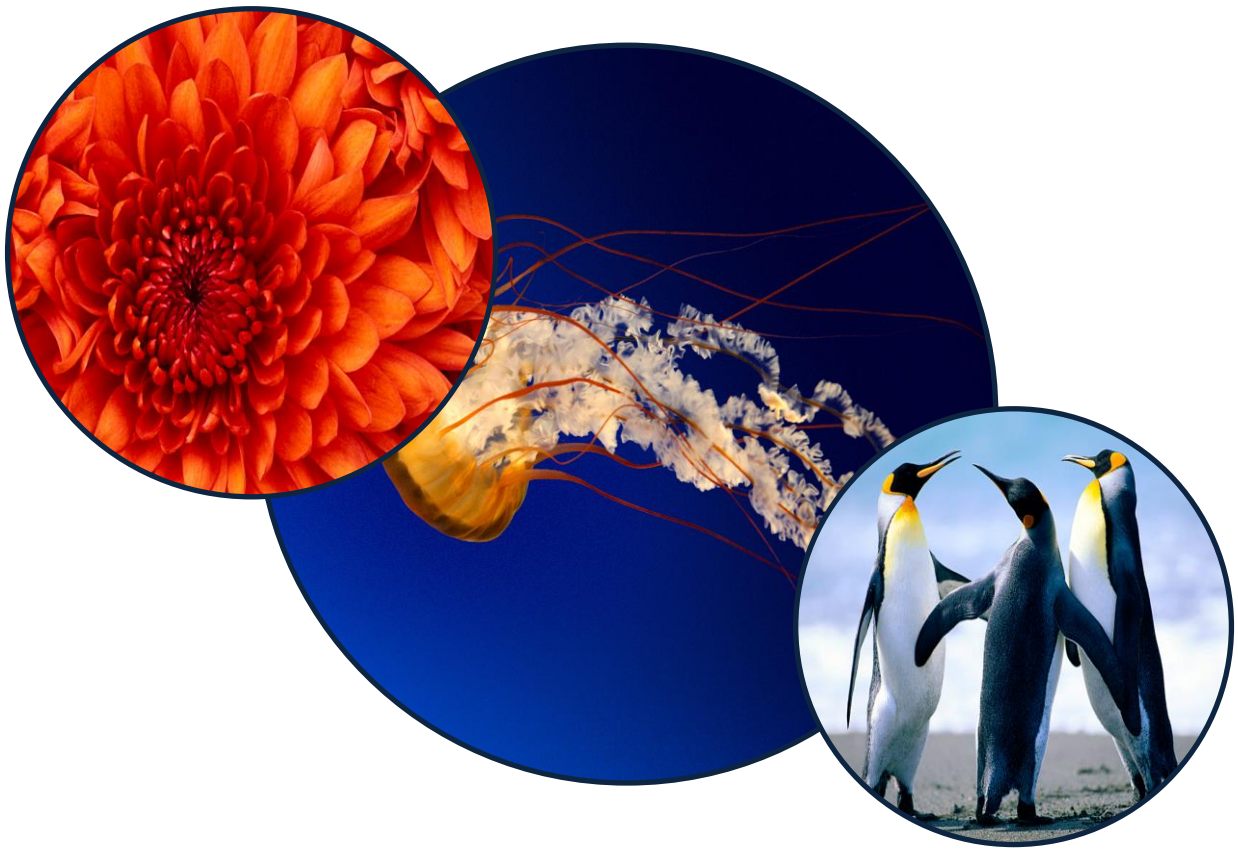
Studie nr. 20 20 67 43
Kort nr. 18 98 87

**MASTERPROJEKT**

**LINIE: ORGANISATION**

# UNDERSØGELSE AF INTERNET OF THINGS (IOT-ENHEDER) OG SIKKERHED I HJEMMET

Daniel Ellebæk, maj 2023



rapport / maj 2023

# Abstract

This report examines the impact of Internet of Things (IoT) devices on Information Technology (IT) security within Danish homes and businesses. IoT devices, widely embedded in the form of smartphones, tablets, gaming consoles and other forms, contain software of varying security levels. Despite their diverse functionalities, they pose significant IT security challenges due to outdated software and other inherent vulnerabilities.

Motivated by a growing interest and gap in the field of IT security, this study focuses on how these IoT devices influence IT security. A handful of commonly used IoT devices are assessed through literature reviews to identify potential weaknesses and their contribution to security compromise.

With the increasing tendency of remote work, particularly propelled by the Coronavirus pandemic, there is a pressing need to examine the safety of home workplaces. As the presence of IoT devices increases, questions around the comparability of security levels across devices like smart TVs and smart bulbs arise. The study hypothesizes that IoT devices are lowering IT security in Danish homes and making home workplaces more vulnerable.

The report presents data on remote work prevalence, explains the IoT concept, undertakes a systematic literature review, and discusses security measures as per ISO 27001. This project aims to examine the extent of the threat posed by IoT devices in Danish homes and their implications, focusing particularly on the security of home workplaces.

As such, the key research question is: How are IoT devices in Danish homes a threat to IT security, and how can they be secured? Through this investigation, the report contributes to a deeper understanding of the complexities of IoT device security, ultimately aiming to increase attention to digital system protection.

The main conclusions drawn from this report are that IoT devices in Danish homes can pose serious security threats, including the risk of cybercriminals gaining access to sensitive information. To enhance security, key measures such as increased education and awareness on IT security, improved IoT architecture, regular software updates, and the use of strong passwords and two-factor authentication were emphasized. Additionally, the importance of standardizing security standards for IoT devices was underscored, as it will contribute to higher security levels and user convenience. This research underscores the urgent need for continuous research in this ever-evolving field to develop effective solutions and build a secure IT infrastructure within Danish households.

# Abstrakt

Denne rapport undersøger virkningen af IoT-enheder (Internet of Things) på informationsteknologi (IT) sikkerhed i danske hjem og virksomheder. IoT-enheder, som er vidt udbredt i form af smartphones, tablets, spillekonsoller og andre former, indeholder software med varierende sikkerhedsniveauer. På trods af deres forskellige funktioner, udgør de betydelige IT-sikkerhedsudfordringer på grund af forældet software og andre iboende sårbarheder.

Motiveret af en voksende interesse og et hul i IT-sikkerhedsfeltet, fokuserer denne undersøgelse på, hvordan disse IoT-enheder påvirker IT-sikkerheden. En håndfuld almindeligt anvendte IoT-enheder vurderes gennem litteraturgennemgang for at identificere potentielle svagheder og deres bidrag til kompromittering af sikkerheden.

Med den stigende tendens til fjernarbejde, især fremmet af Coronavirus-pandemien, er der et presserende behov for at undersøge sikkerheden af hjemmearbejdspladser. Da tilstedeværelsen af IoT-enheder øges, opstår spørgsmål om sammenligneligheden af sikkerhedsniveauer på tværs af enheder som smart TV og smarte pærer. Undersøgelsen antager, at IoT-enheder sænker IT-sikkerheden i danske hjem og gør hjemmearbejdspladser mere sårbare.

Rapporten præsenterer data om udbredelsen af fjernarbejde, forklarer IoT-konceptet, foretager en systematisk litteraturgennemgang, og diskuterer sikkerhedsforanstaltninger i henhold til ISO 27001. Dette projekt har til formål at undersøge omfanget af den trussel, som IoT-enheder i danske hjem udgør, og deres implikationer, med særlig fokus på sikkerheden af hjemmearbejdspladser.

Således er det centrale forskningsspørgsmål: Hvordan er IoT-enheder i de danske hjem en trussel imod IT-sikkerheden, og hvordan skal de sikres? Gennem denne undersøgelse bidrager rapporten til en dybere forståelse af kompleksiteten i IoT-enhedssikkerhed, med det ultimative formål at øge opmærksomheden på beskyttelse af digitale systemer.

De vigtigste konklusioner trukket fra denne rapport er, at IoT-enheder i danske hjem kan udgøre alvorlige sikkerhedstrusler, herunder risikoen for at cyberkriminelle får adgang til følsomme oplysninger. For at forbedre sikkerheden er nøgleforanstaltninger såsom øget uddannelse og bevidsthed om IT-sikkerhed, forbedret IoT-arkitektur, regelmæssige softwareopdateringer, og brugen af stærke adgangskoder og to-faktor-autentificering understreget. Desuden er vigtigheden af at standardisere sikkerhedsstandarder for IoT-enheder understreget, da det vil bidrage til højere sikkerhedsniveauer og brugerbelejlighed. Denne forskning understreger det presserende behov for kontinuerlig forskning på dette konstant udviklende felt for at udvikle effektive løsninger og bygge en sikker IT-infrastruktur i danske husstande.

# Indholdsfortegnelse

# 1 INTRODUCERENDE AFSNIT

## 1.1 INDLEDNING

IoT-enheder (Internet of Things) findes i stort set alle danske hjem i form af smartphones, tablets, spillekonsoller og mange andre afskygninger. IoT-enheder beskrevet som ”ting” som er på internettet med følere, scannere, kameraer eller f.eks. sensorer. Det er ikke kun de danske hjem, som tilføjer nye IoT-enheder hvert år, men i stor stil også i de danske virksomheder. Udover det er spændende at se en voksende tendens, er det også relevant at se på, hvilke fordele og ulemper tendensen tager med sig.

Selvom mange IoT-enheder er sikre i den forstand, at de ikke brænder sammen, kan disse indeholde software som er mere eller mindre usikkert. Enhedernes sikkerhed er ikke bedre end det software, som de er fabrikeret med, og i nogle tilfælde er der tale om forældet software. Dette er med til at forringe IT-sikkerheden, men hvor slemt står det faktisk til?

Denne rapport vil indskrænke undersøgelsen til danske virksomheder og hjems IoT-enheder. En håndfuld kendte IoT-enheder vil blive betragtet og undersøgt for at finde svagheder, og hvordan enhederne bidrager til at kompromittere IT-sikkerheden.

## 1.2 HVORFOR EKSISTERER DETTE PROJEKT?

Dette projekt er blevet udarbejdet på baggrund af en interesse og et ufuldendt område inden for IT-sikkerheden. IoT-enheder breder sig alle steder, og får en større betydning i alles hverdag. De fleste tænker måske ikke så meget over hvad IoT-enheder faktisk er og gør, eller med hvilke implikationer de kan have på IT-sikkerheden. Det er derfor spændende at undersøge, hvordan IoT-enheder påvirker IT-sikkerheden. En ting som umiddelbart virker relativt klart ift. artikler og udtalelser fra eksperter og sikkerhedsvirksomheder er, at IoT-enheder ikke nødvendigvis bidrager med at sikre opretholdensen af IT-sikkerhed [1].

## 1.3 FORMÅL MED PROJEKTET OG VURDERING AF DETS BETYDNING (HYPOTESE)

Formålet med projektet er at undersøge IoT-enheder i de danske hjem og hvordan de påvirker IT-sikkerheden. Der har været en stigende tendens for hjemmearbejde, og specielt i 2020-2021 da Coronavirus tvang de fleste danskere til at arbejde hjemmefra. Er danskernes hjemmearbejdspladser sikre nok til at være arbejdspladser, eller er der et helt andet behov?

Betydningen af den stigende tendens for IoT-enheder betyder også, at der er flere enheder på internettet, og er sikkerheden lige god i et smart TV til f.eks. en smart pære? Det kan være afgørende at få et klarere syn på, hvordan IoT-enheder påvirker it-sikkerheden, da dette kan bidrage til at øge opmærksomheden omkring beskyttelse af digitale systemer.

Hypoteserne i denne rapport er følgende:

Hypoteser (teori):
IoT-enheder er med til at sænke IT sikkerheden i de danske hjem.
IoT-enheder er med til at gøre de danske hjem mere usikre hjemmearbejdspladser.
Danskernes hjemmearbejdspladser bringer IT-sikkerheden i fare.

## 1.4 PRÆSENTATION AF DATA

For at kunne besvare de forskellige hypoteser samt komme i mål med problemformuleringen nedenfor er det nødvendigt, at præsentere den data, som bliver brugt igennem rapporten. Præsentation af data er i følgende rækkefølge:

1. Hjemmearbejde og udbredelse
2. Hvad er IoT
3. Systematisk Litteratur Review
4. Sikkerhedstiltag ved ISO 27001

## 1.5 PROBLEMFORMULERING

IoT-enheder fylder mere og mere i de danske hjem. Den danske forbruger modtager en stor bunke reklamer om smarte hjem, smarte TV, smart lys og andre IoT-enheder på daglig basis igennem deres e-mails, normal post og på reklametavler. Ud over de faste IoT-enheder som smartphones, tablets, labtops osv. er der kun flere og nye af slagen, som venter på at blive købt af den danske forbruger. De store forretningskæder som Power og Elgiganten reklamerer og har udstillinger om hvor let forbrugerens hverdag kan blive ved at installere og købe flere IoT-produkter. Set ud fra forretningskædernes øjne forsøger de, at vise den danske forbruger til at blive mere smart i deres hjem ergo købe flere IoT-enheder. Dette er med til at sikre, at flere enheder kommer på internettet, og øger den tekniske kompleksitet drastisk.

Udviklingen spår, at der kommer til at være mange flere IoT-enheder i de danske hjem end der hidtil har været. Dette bekymrer de danske IT-sikkerhedsvirksomheder, som bl.a. udtaler, at IT-sikkerheden hænger i en rød tråd, men at der stadigvæk er håb forude.

Derfor vil dette projekt bl.a. fokusere på at undersøge, hvor stor en trussel IoT-enheder er i de danske hjem og med hvilke implikationer de har, og undersøge om hjemmearbejdspladserne har været en trussel imod IT-sikkerheden.

---

*Hvordan er IoT-enheder i de danske hjem en trussel imod IT-sikkerheden, og hvordan skal de sikres?*

---

## 1.6 PRÆSENTATION AF METODE OG FREMGANGSMÅDE

Udfordringerne med IT-sikkerhed i danske hjem intensiveres af en mangel på teknisk ekspertise, og parallelt hermed, en stigende tendens til at anskaffe IoT-enheder. Denne situation stiller det danske samfund over for betydelige udfordringer i forhold til IT-sikkerhed. For at afdække om IoT-enheder udgør en trussel mod IT-sikkerheden, anvendes et systematisk litteratur review som metode.

Ved at gennemgå en række relevante forskningsartikler og analysere, om der er identificeret nogen sårbarheder i studierne, bidrager dette til at kaste lys over problemstillingen. Resultaterne af det systematiske litteratur review anvendes til at formulere en række anbefalinger for forbedring af IT-sikkerheden.

Andet afsnit indledes med en undersøgelse af begrebet IoT-enheder, som repræsenterer et netværk af fysiske objekter, udstyret med sensorer, software og andre teknologier, der har til formål at forbinde og udveksle data med andre enheder og systemer over internettet.

Tredje afsnit i rapporten fokuserer på hjemmearbejde og den øgede udbredelse af dette fænomen. Udbredelsen og den deraf følgende øgede brug af teknologi i hjemmet belyses, da det har betydning for den samlede IT-sikkerhed.

I det fjerde afsnit udføres et systematisk litteratur review, hvor relevante forskningsartikler identificeres og analyseres. Disse artikler har undersøgt potentielle sårbarheder i IT-sikkerheden, særligt med hensyn til brugen af IoT-enheder.

Rapportens femte afsnit præsenterer sikkerhedstiltag, som kan implementeres i hjemmet for at forbedre IT-sikkerheden. Disse anbefalinger er baseret på fundene fra det systematiske litteratur review og har til formål at vejlede læseren i at forbedre sikkerhedsforanstaltningerne i forbindelse med anvendelsen af IoT-enheder.

Til sidst frembringes en konklusion, hvor hovedpunkterne fra de foregående afsnit opsummeres, og der reflekteres over rapportens indhold og de fremlagte resultater. Denne del fungerer som et afsluttende element, der samler og tydeliggør rapportens hovedargumenter og fund.

# 2 HVAD ER IOT

IoT eller Internet of Things er enheder som er koblet op til internettet, som altid eller delvist er online, og sender signaler til onlineservere eller kommunikere med andre enheder i hjemmet, på arbejdspladsen eller i det offentlige rum. En IoT-enheds primære job er, at løse det som enheden er designet til at gøre. Dette kunne være at støvsuge et værelse eller måske at sende beskeder til applikationer installeret på smartphones vedr. mangler i køleskabet. Der er stort set ingen grænser for hvilke IoT-enheder der ikke er udviklet, og sælges online på f.eks. Amazon eller AliExpress. Til fælles for alle IoT-enheder er, at de er koblet op til internettet, og at de sender data frem og tilbage imellem servere og andre enheder.

For bedre at kunne give et overblik over hvad IoT-enheder er, og hvilke slags enheder der faktisk findes på internettet, er denne nedenstående illustration (Figur 1) taget i brug:

**Figur 1 - https://www.nist.gov/sites/default/files/images/2020/05/29/shutterstock_520084003.jpg**

Figur 1 viser en oversigt over IoT-enheder som i dag kan findes på internettet. Det ses meget tydeligt, at de enheder som er koblet op til internettet, kan være hvad som helst lige fra termometre, sikkerheds kameraer, biler eller f.eks. en potteplante.

Umiddelbart er IoT-enheder som en dejlig og fantastisk ting at have i hjemmet eller på arbejdspladsen. Men følgende spørgsmål forbliver relevante:

*Er IoT-enheder sikre at benytte over internettet?*

*Kan forbrugere stole på, at fabrikanten har sikret kommunikationen med den bedste og nyeste kryptering?*

Svaret på de to spørgsmål kan umiddelbart besvares med enkelte ord, da der allerede findes en masse historik fra tidligere IoT-enheder. Men er det altid sådan at billedet skal tegnes, eller er IoT-enheders fabrikanter blevet bedre med tiden, og begyndt at tænke mere over sikkerheden?

I denne rapport vil der blive kigget på sikkerheden ved IoT-enheder, ved at undersøge den nyeste forskning.

## 2.1 EKSEMPLER PÅ IOT-ENHEDER

Her vises eksempler på IoT-enheder fundet på Amazon. Denne sektion har til formål, at vise og give læseren en forståelse af IoT-enheders udbredelse ved at vise faktuelle produkter.

### 2.1.1 ALEXA LYS PÅ WIFI


Intelligente lys som er koblet op til internettet, kan styres let og enkelt igennem stemmestyring med Alexa eller via en applikation som installeres direkte på smartphones. Alexa er en stemmestyret IoT-enheder, som fungerer som en slags søgemaskine, og kan let styre ens smarte lys.

Med sådanne smarte lys er det let og lige til, at slukke og ændre lysstyrken i hjemmet. På mange måder giver dette en fornemmelse for fremtid og det smarte hjem.


Som det også ses på billederne, er det let, og lige til at benytte. Der bliver lagt vægt på at reklamere til forbrugere om dette produkt, som noget der kan hjælpe og gøre hverdagen lettere.

For de fleste forbrugere ville det sandsynligvis virke behageligt at have et apparat i hjemmet, som kan tales til – noget, der har været skildret i film siden 1960'erne.

### 2.1.2 SMART TV

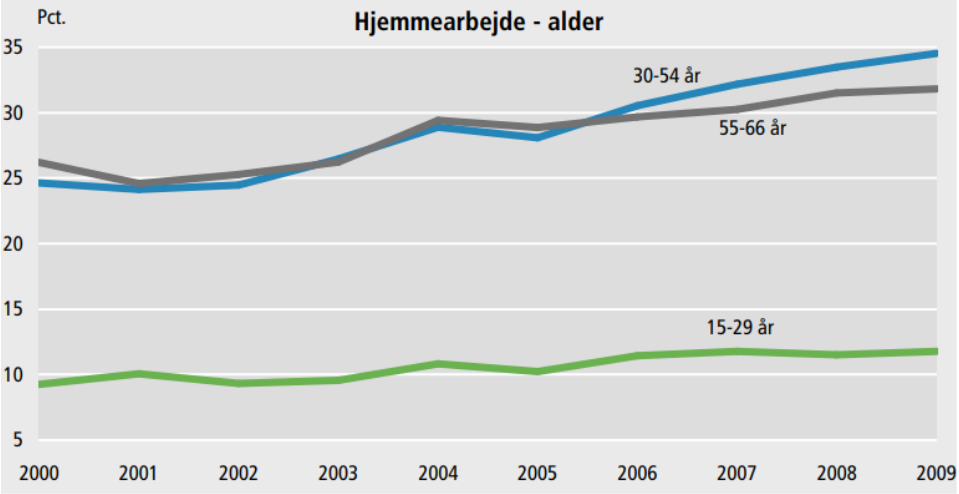

Smarte TV har eksisteret i mange år, og er kommet for at blive. Et smart TV kommunikeres med igennem infrarøde signaler fra en fjernbetjening. Disse signaler får TV'et til at reagere. Men før alt dette kan ske skal TV'et forbindes til internettet.

Et smart TV har applikationer installeret på sig, får firmware opdateringer, og med få klik kan alt streames direkte fra smartphones til TV.
Til fælles har begge IoT-enheder de samme features, som består af at være tilkoblet internettet, og tilbyde funktioner til forbrugeren for at gøre brugen af dem lettere.

# 3 HJEMMEARBEJDE OG UDBREDELSE

## 3.1 HJEMMEARBEJDE OG UDBREDELSE ÅR 2000 - 2009

Flere og flere benytter sig af muligheden for at arbejde hjemme, og helt op imod 33% har benyttet sig af muligheden for at arbejde hjemmefra i de brancher hvor en internetforbindelse var det eneste krav. Det at arbejde hjemme bliver anset som en medarbejdergode hvor ens chef skal have tillid til medarbejderen. Det er komfortabelt at arbejde hjemmefra bl.a. kan der spares på rejsebilletten, og tiden der benyttes til og fra arbejdet. Det er lettere at have en hjemmearbejdsstation da teknologien er blevet bedre f.eks. i form af bedre kameraer, mikrofoner, computere og ikke mindst internetforbindelser. En meget vigtig del af hjemmearbejde er internettet da de fleste arbejdsopgaver som regel kræver internet. Det ses også at meget af det arbejde er findes på arbejdsmarkedet er mere projektorienteret, hvilket giver en bedre mulighed for at arbejde hjemmefra. Igen styrker arbejdsmarkedet muligheden for at give hjemmearbejde flere ben at stå på. [2]




**Figur 2 - Hjemmearbejde alder fra år 2000-2009 https://www.dst.dk/-/media/Kontorer/16-Formidlingscenter/Bag-Tallene/2010/2010-02-24-hjemmearbejde-pdf_001-pdf.pdf**

Illustrationen på Figur 2 viser i årstal fra år 2000 til og med år 2009 at der er en stigende tendens i hjemmearbejde. Der er også en stor forskel på hvilke brancher som arbejder hjemmefra. Branchen med den største andel hjemmearbejdende er *Information og Kommunikation* (se Figur 3) som dækker over halvdelen (54%), som har arbejdet hjemme mindst en gang. Dette bakker op omkring at brancher med programmører og sælgere i en stigende grad ses som et job med mere og mere hjemmearbejde.

| | 2009 |
|---|---|
| | — Pct. — |
| Landbrug, skovbrug og fiskeri | 43 |
| Industri, råstofudvinding og forsyningsvirksomhed | 22 |
| Bygge og anlæg | 22 |
| Handel og transport mv. | 18 |
| Information og kommunikation | 54 |
| Finansiering og forsikring | 32 |
| Ejendomshandel og udlejning | 37 |
| Erhvervsservice | 41 |
| Offentlig administration, undervisning og sundhed | 32 |
| Kultur, fritid og anden service | 31 |

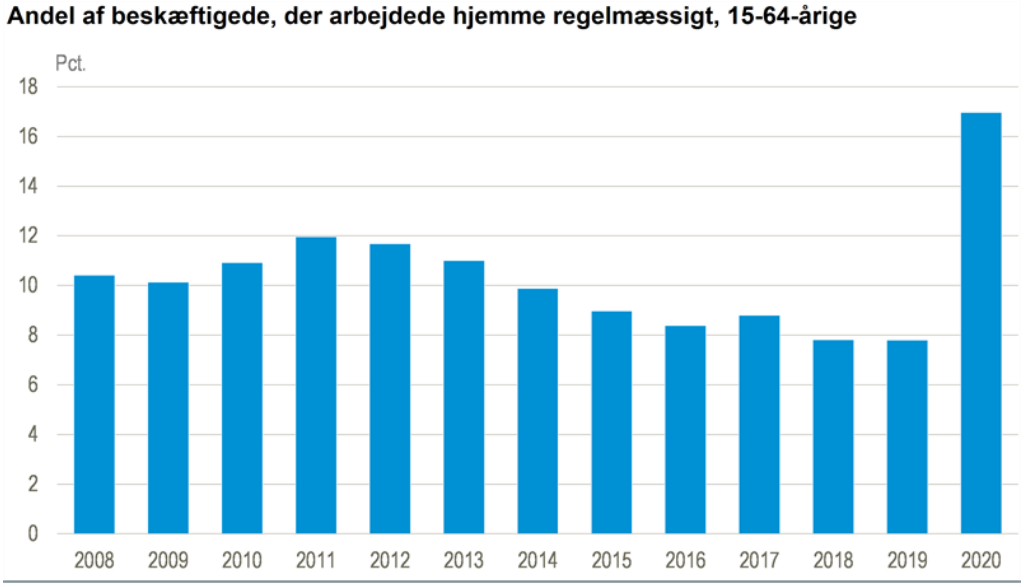
**Figur 3 - Andel med hjemmearbejde fordelt på brancher https://www.dst.dk/-/media/Kontorer/16-Formidlingscenter/Bag-Tallene/2010/2010-02-24-hjemmearbejde-pdf_001-pdf.pdf**

Samlet set viser udviklingen fra år 2000 og frem til år 2009 at være i stigning.

## 3.2 HJEMMEARBEJDE OG UDBREDELSE ÅR 2020

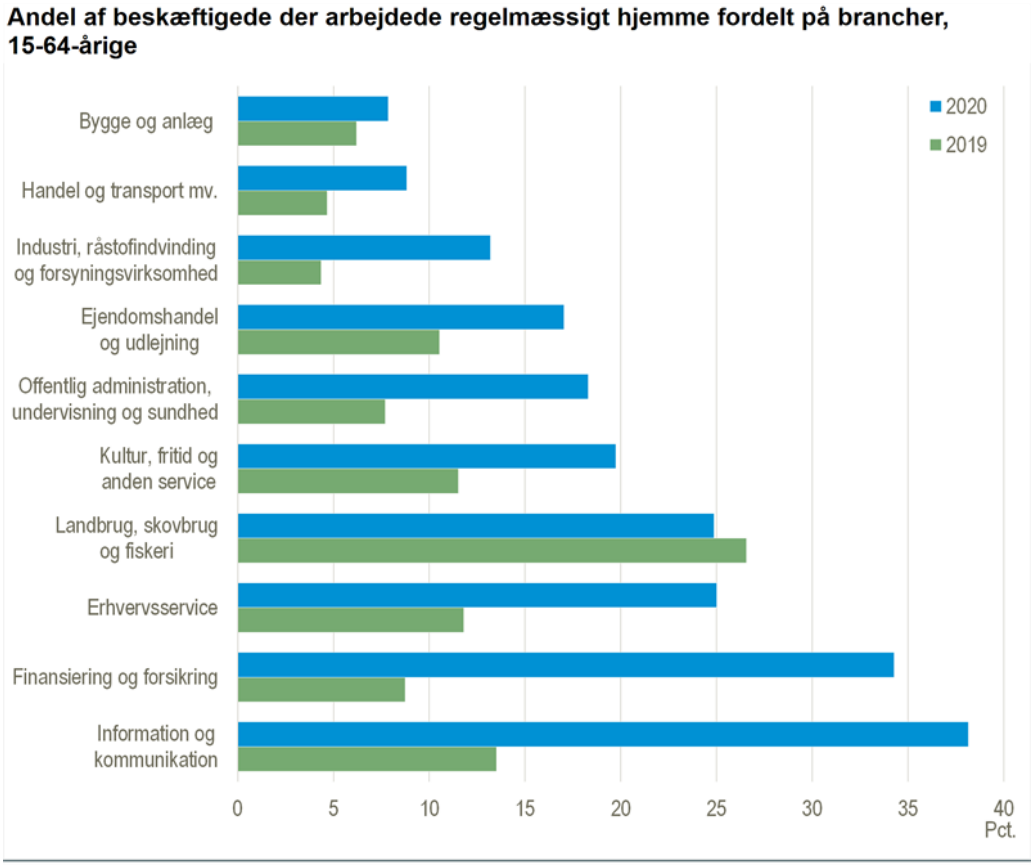
Udviklingen af hjemmearbejde fra år 2000 og frem til år 2009 er stigende, hvorfor det netop er spændende at se 10 år efter om tendensen stadigvæk er stigende. Data fra før år 2000 kan være relevante men i forhold til denne opgave er det en tendens der ønskes oplyst, som gerne skal repræsentere nutiden.

I år 2020 arbejdede 17% af beskæftigede hjemme regelmæssigt hvilket er en fordobling fra året før som også er den højeste registreret mængde af hjemmearbejde nogen sinde. Det er vigtigt at fremhæve COVID-19 pandemien da rigtig mange danskere blev hjemsendt i en længere periode i 2020. Rettes blikket imod Figur 4 ses det at der både i 2018 og 2019 andelsmæssigt var 8% arbejdende hjemmefra. I 2011 topper hjemmearbejdet med hele 12% før pandemien starter i år 2020. Statistisk set viser tendensen en nedgang i hjemmearbejde fra år 2012 frem til 2020.




**Figur 4 - Andel af beskæftigede, der arbejdede hjemme regelmæssigt, 15-64-årige https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=32435**

De forskellige brancher havde en stigning ift. hjemmearbejde som en konsekvens af COVID-19 pandemien. Dette ses på Figur 5. I år 2020 arbejdede 38% hjemme inden for branchen *Information og Kommunikation* som er en stigning på 24 procentpoint i forhold til 2019. Igen skal det huskes at dette er en direkte konsekvens af COVID-19 pandemien. Stort set alle andre brancher havde en stigning af hjemmearbejde under COVID-19 pandemien lige med undtagelse af *Landbrug, Skovbrug og fiskeri*. [3]




**Figur 5 - Andel af beskæftigede der arbejdede regelmæssigt hjemme fordelt på brancher 15-64-årige https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=32435**

## 3.3 HJEMMEARBEJDE ER MERE UDBREDT END FØR COVID-19

Mængden af hjemmearbejde steg drastisk under COVID-19 pandemien som f.eks. kom til syne ved Information og Kommunikation steg med 48 procentpoint, se Figur 6. Dette mønster ses ved stort set alle brancher, men helt tydeligt er det, at mængden af hjemmearbejde endnu ikke er nede på det niveau, det var før pandemien marts 2020. Kigges der på andre brancher Kultur, fritid og anden service var der 10.2% hjemmearbejde før pandemien, og hele 26.7% under pandemien. Mængden af hjemmearbejde faldt til 14.2% efter pandemien som er en forskel på 4%. Denne udvikling kan igen ses på stort set alle brancher.

Det kan derfor konkluderes at mængden af hjemmearbejde efter COVID-19 pandemien er steget en smule. Årsagen til dette kunne f.eks. være, at der efter en længere periode med hjemmearbejdet er kommet bedre fokus på hvilke typer af jobs der kan udføres i hjemmet, og at arbejdspladsen har åbnet for muligheden. Om denne stigning i løbet af næste år vil forsætte eller stabiliseres er spændende ift. udviklingen, og hvis der fortsat er en stigning, betyder det også, at der med stor sandsynlighed bliver stillet flere krav til bl.a. IT-sikkerheden og udstyr i hjemmet.

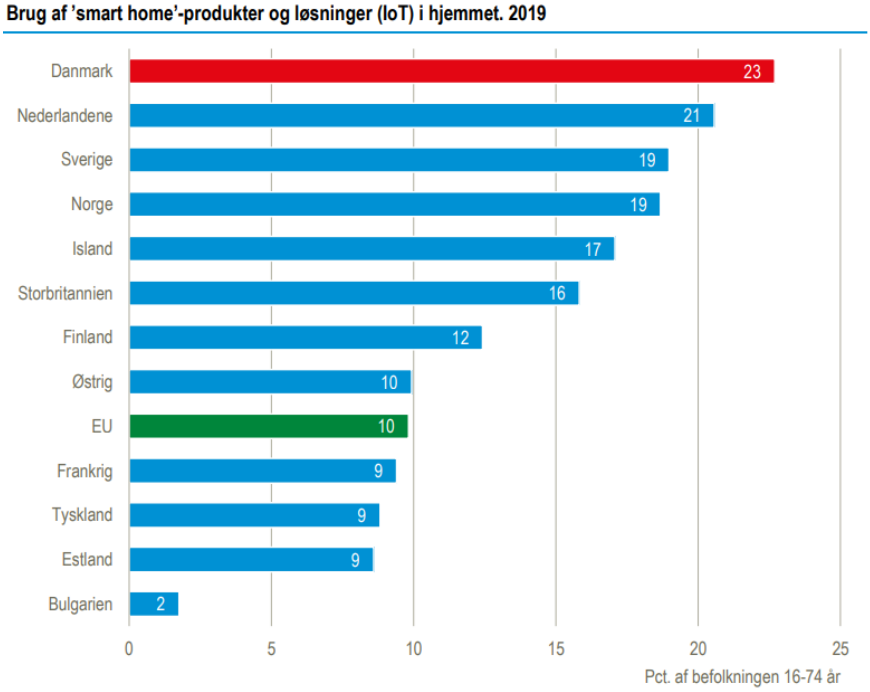
**Andel af hyppigt hjemmearbejde fordelt på brancher, 15-64 år.**

| | 2. kvt. 2019 | 2. kvt. 2020 | 2. kvt. 2021 | 2. kvt. 2022 |
|---|---|---|---|---|
| | pct. | | | |
| Landbrug, skovbrug og fiskeri | 28,0 | 26,2 | 21,5 | 23,3 |
| Industri, råstofudvinding og forsyningsvirksomhed | 5,2 | 20,4 | 14,8 | 7,7 |
| Bygge og anlæg | 6,8 | 10,5 | 6,3 | 5,8 |
| Handel og transport mv. | 4,7 | 11,5 | 10,6 | 7,2 |
| Information og kommunikation | 14,0 | 58,0 | 49,7 | 31,9 |
| Finansiering og forsikring | 8,4 | 51,1 | 50,0 | 18,2 |
| Ejendomshandel, udlejning og erhvervsservice | 11,5 | 35,7 | 26,4 | 16,3 |
| Offentlig administration og undervisning | 9,0 | 51,1 | 36,9 | 12,6 |
| Sundhed | 5,7 | 15,5 | 9,8 | 6,4 |
| Kultur, fritid og anden service | 10,2 | 26,7 | 24,9 | 14,2 |

**Figur 6 - Andel af hyppigt hjemmearbejde fordelt på brancher, 15-64-årige https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=40158**

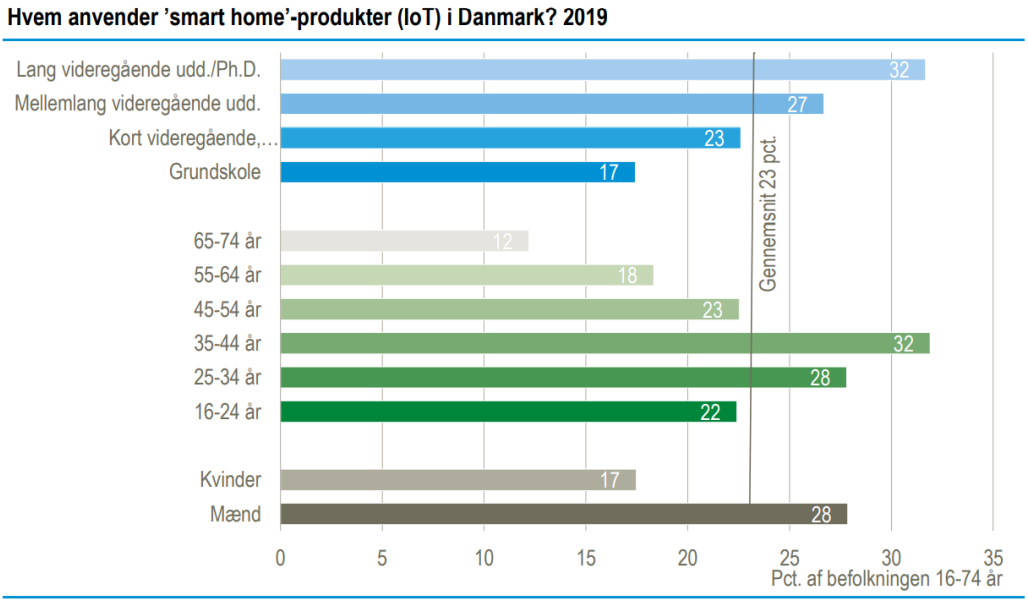
## 3.4 IOT-ENHEDER ER EN STIGENDE TENDENS

Når det kommer til anvendelsen af IoT-produkter havde Danmark rekord i brug af 'smart home '-produkter i år 2019 med hele 23%, af danskerne som havde brugt en eller flere enheder, illustreret på Figur 7. De mest udbredte IoT-enheder var Smarte elpærer, alarmsystemer, musikafspillere, termostater, stemmestyrede personlige 'assistenter', badevægte, robot-støvsugere og -plæneklippere, som alle fandt vejen til hjemmet. [4]




**Figur 7 - Brug af 'smart-home '-produkter og løsninger (IoT) i hjemmet 2019 https://www.dst.dk/Site/Dst/Udgivelser/nyt/GetPdf.aspx?cid=36216**

Når undersøgelsen af, hvem der benytter IoT-enheder (se Figur 8 , foretages, udgør mænd en større andel. Ud over køn er der også forskel på aldersgrupper hvor dem med en lang videregående uddannelse/Ph.d. udgør den gruppe med størst anvendelse. Med denne information er det muligt at sige, at IoT-enheder i den grad bliver benyttet i Danmark, og har en stigende tendens iblandt unge og dem som ligger i aldersgruppen 35-44 år.




**Figur 8 - Hvem anvender 'smart home '-produkter (IoT) i Danmark? 2019**
**https://www.dst.dk/Site/Dst/Udgivelser/nyt/GetPdf.aspx?cid=36216**

#### *3.4.1.1 Hvad er 'smart home '-produkter?*

Blandt 'smart home '-produkter findes der et utal af produkter, som findes i de danske hjem. F.eks. kan højtalere, støvsugere, kaffemaskiner, lamper, alarmsystemer og kobles på internettet. En sådan opkobling gør det muligt for disse enheder, at sende og modtage data f.eks. igennem en smartphone. På den måde er det muligt at styre produktet enten med kommandoer fra en app eller f.eks. med stemmestyring. Det er forskelligt hvor intelligente produkterne er, i nogle tilfælde kan produktet tales til, og på den måde opfange en kommando. Det betyder som sådan ikke så meget hvilket produkt, som kategoriseres som IoT-enhed, da de alle har den samme mulighed "at blive tilsluttet internettet". Når en IoT-enheder tilkobles internettet er det software i enhederne, som bestemmer funktionalitet. Derfor er det ikke så vigtigt, om der tales om køleskabe eller smarte lyskugler til juletræet – det går ud på det samme.

## 3.5 UDTALELSER VEDR. RISICI VED IOT-ENHEDER

Med en stigende tendens af IoT-enheder i hjemmet følger der også et stigende antal hackerangreb imod disse enheder. I år 2020 var der en stigning på 50% [5] i første halvår af angreb imod IoT-enheder. Årsagen til den stigende tendens inden for hackerangreb har rødder i, at mange fabrikanter ikke tager sikkerheden alvorligt (nok?). Når danskerne installerer kameraer eller smartlåse i deres hjem bliver det ganske enkelt forventet af forbrugeren at sikkerheden er i orden, desværre er det langt fra tilfældet.

Spørgsmålet om, hvad hackere skal i danskernes IoT-enheder, er blevet stillet mange gange. Her er svaret langt fra atypisk i forhold til at hackerne enten går efter personlige informationer eller ønsker at benytte IoT-enheden til deres botnet eller anden IT kriminel handling.

Et botnet er en betegnelse for et netværk af enheder, hvis computerkraft kan benyttes i et angreb som hackerne kontrollere. En kendt type angreb som ses botnet udfører er det såkaldte DDoS-angreb, som

giver hackerne mulighed for, at oversvømme en server med store mængder af trafik, som kan have til følge at serveren holder op med at virke eller bliver lagt ned [6].

I 2021 viste en undersøgelse foretaget af HP Hewlett-Packard at en ud af 12 ansatte på kontorer har været ramt af en virus eller udsat for et phishingangreb eller på anden vis fået deres arbejdscomputer hacket. Generelt viste undersøgelsen fra HP at der stigning af hackerangreb under COVID-19 pandemien, samtidig med at de angreb hackerne udførte var blevet mere sofistikerede. Et populært angreb var det gamle velkendte phishing-angreb, som blev forklædt som fakturaer med formål at skaffe sig adgang til de ansattes enheder eller franarre virksomhedernes forretningskritiske oplysninger.

På hjemmearbejdspladserne var angrebet phishing meget succesfuldt for hackerne, da der ligger noget trygt i at arbejde hjemme fra, som er med til at sænke medarbejderens parader og beskyttelse som på arbejdspladsen [7].

Helt typisk havde COVID-19 pandemien også lagt nogle spor efter sig. Under COVID-19 pandemien blev der udført meget hjemmearbejde, hvilket gav danskerne en mulighed for at lære om IT-sikkerhed i hjemmet. De, som var i en gunstig situation, modtog vejledninger fra deres arbejdsplads. Med dette menes der, at danskerne i stor grad selv måtte stå for IT sikkerheden, og dette har ført med sig, at op til 67% føler sig bekymret over deres onlinesikkerhed. Dette er delvist forståeligt, da under COVID-19 pandemien skiftede ansvaret for cybersikkerhed pludselig fra virksomhederne til den enkelte danskers skuldre [8].

## 3.6 AFKLARING

IoT-enheder er kommet for at blive. Men der tegnes et tydeligt billede af, at IoT-enheder ikke er fabrikeret med mange sikkerhedsfeatures, som giver forbrugeren den nødvendige beskyttelse imod cyberangreb. Alt dette bliver bl.a. oplyst igennem private undersøgelser, som viser at offentligheden er klar over den stigende tendens af antallet af IoT-enheder, og på samme tid kender til sårbarhederne. Desværre kan det nok ikke siges, at den almene dansker skal have forstand på sikkerheden i sådan et omfang, at sikkerheden er noget alle tager sig af. Derfor er det nødvendigt at få fabrikanterne med. Fabrikanterne skal implementere sikkerhed i et langt større omfang, og med fokus på hvilke foranstaltninger samt hvilke sårbarheder, der er nødvendige. Dette er noget som der vil blive belyst i den systematiske litteratur Review over IoT-enheder og sårbarheder.

# 4 SYSTEMATISK LITTERATUR REVIEW AF IOT-ENHEDER OG SÅRBARHEDER

Formålet med dette systematiske litteratur review er at samle og overskueliggøre relevante forskningsresultater for på den måde at besvare problemformuleringen.

## 4.1 AFGRÆNSNING AF PROJEKTET

Siden år 2009 har der været en stigning i hjemmearbejdet. Dette kom for alvor til syne under COVID-19 pandemien, da virksomheder pludseligt skulle finde en løsning på hjemmearbejdskontoret. Hjemmearbejdskontoret var arbejdspladsen for rigtigt mange mennesker i hele verden, og specielt i de brancher hvor en internetforbindelse var det eneste krav. Der er et stort forskningsområde i de sidste par år som kan afdække behovet for hjemmearbejde, og med hvilke foranstaltninger skal virksomhederne kræve til deres medarbejdere for at sikre en sikker hjemmearbejdsplads.

Dette projekt vil give et mere tydeligt billede af hvordan IoT-enheder er en trussel, når den almene dansker tager arbejdet med hjem. Hjemmearbejdspladser er blevet meget accepteret, og er i en stigende grad noget som stadigvæk er en virkelighed. Hvordan skal disse hjemmearbejdspladser sikres på den bedst tænkelige måde, og er der nogle krav virksomheden kan stille til deres medarbejdere. For bedst muligt at kunne komme i mål med denne rapport afgrænses projektet til at besvare problemformuleringen ud fra en mindre antal forskningsartikler, som nøje er blevet udvalgt netop til formålet.

## 4.2 METODE TIL UDVÆLGELSE AF FORSKNINGSARTIKLER

Med hensyn til valg af database til søgning efter relevante forskningsartikler var IEEE og ACM i betragtning. ACM peger mest imod datalogi/data science hvor IEEE primære områder er elektriske systemer inden for ingeniørområdet med fokus på hardware, telekommunikation og kredsløb.

Databasen IEEE har en bedre beskrivelse ift. snittet af rapportens problemstilling samtidig med den et bredere søgningsgrundlag. Derfor blev denne valgt.

Det blev besluttet at alle søgninger skulle være rettet imod titlen og ikke en fuldtekstsøgning. Årsagen til dette er, at titlen gerne skulle indeholde de mest relevante ord som forskningsartiklerne omhandler. F.eks. hvis titel var ” Vulnerabilities in IoT devices” ville den være meget relevant ift. dette projekt. Der kan i en fuldtekstsøgning tit forekomme de søgekriterier som er opstillet f.eks. ord som IoT eller vulnerability, men dette betyder ikke, at artiklen direkte omhandler IoT-enheder og sårbarheder. Derfor er titlen mere suveræn og er blevet brugt som et direkte kriterie.

Da problemformuleringen spørger ind til hvordan IoT-enheder er en trussel og hvordan de sikres, har det været relevant at finde passende søgekriterier, som gav en mængde forskningsartikler, som var i direkte relevans. Disse søgekriterier var:

1. IoT AND vulnerability

Forståelse af søgekriterier:

| Terminologi | Forklaring |
|---|---|
| **IoT** | IoT står for Internet of Things. |
| **vulnerability** | Vulnerability betyder sårbarhed. |

Årsagen til at vælge IoT og vulnerability som søgekriterier var at finde flest mulige relevante artikler for projektets retning. Det blev besluttet at minimere søgekriterierne for at undgå unødvendig afgrænsning.

Ekstra søgekriterier som blev brugt:

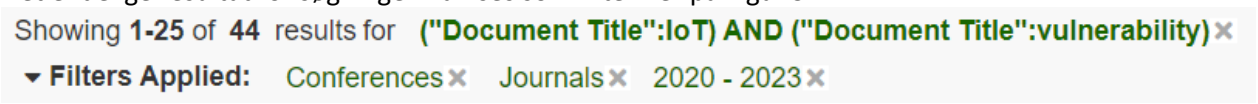
1. Skal være på engelsk
2. Skal være fra år 2020-2023
3. Kun Journals (artikler) og konference papirer

De to ekstra filtre som ses ovenover, er taget med for bl.a. at sikre, at forskningen kunne læses og forstås. Årstallet er afgrænset til 2020-2023 for at få den nyeste forskning inden for IoT, og at forskning inden for IT-området hurtigt forældes. Med forældes menes der, at forskning som er mere end 2 år gammel ikke bliver betragtet i denne rapport.

### 4.3 FORSKNINGSARTIKLER VED SØGNINGEN PÅ IEEE

Originalt set var tanken at sortere alle forskningsartikler efter citering, men det blev efter en grundig gennemgang af resultaterne besluttet, at alle artikler skulle igennem nåleøjet og sorteres efter relevans. Maksimalt inddrages 10 forskningsartikler.

Det endelige resultat for søgningen kan ses som filter her på Figur 9:




Figur 9 – Resultat for søgning da den blev foretaget på IEEE dato 30 januar 2023

Dette er et billede fra søgningen d. 30. januar 2023, og kan være anderledes på et senere tidspunkt. Meningen med oversigten af søgning er blot at illustrere resultatet for søgning på det tidspunkt den blev foretaget.

## 4.4 VALG AF RELEVANTE FORSKNINGSARTIKLER

Processen bag valget er beskrevet i dette afsnit. Her ses den overordnet proces til hvordan udvælgelsen har foregået:

1. Titlen skal have relevans ift. problemformuleringen
2. Resuméet blev læst for relevans
3. Artiklen blev screenet for at sikre den kan bruges

Disse regler blev brugt for at sikre, at kun den relevante forskning blev inddraget. Her ses se artikler som blev inddraget, og som bruges direkte i rapporten i det systematiske litteratur Review:

| Nr. | Forskningsartikel | Reference |
|---|---|---|
| 1 | Detecting Vulnerability on IoT Device Firmware: A Survey | [9] |
| 2 | Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study | [10] |
| 3 | A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices | [11] |
| 4 | Vulnerabilities and Security Issues in IoT Protocols | [12] |
| 5 | IoT Networks: Security Vulnerabilities of Application Layer Protocols | [13] |
| 6 | A Survey on the Security Vulnerabilities of IoT Smart Home Application | [14] |
| 7 | Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider | [15] |
| 8 | Vulnerability Classification of Consumer-based IoT Software | [16] |

### 4.4.1 REVIEW AF (NR. 1): DETECTING VULNERABILITY ON IOT DEVICE FIRMWARE: A SURVEY

Artiklen beskriver de udfordringer, organisationer står over for med hensyn til at beskytte IoT-enheder mod cyberangreb. Der fokuseres på firmware-sikkerhedsanalyse som en afgørende løsning for at afhjælpe softwarefejl, patche sårbarheder og tilføje sikkerhedsfunktioner til IoT-enheder.

IoT-enheder fylder 30% af alle enheder der er forbundet til internettet. Dette betyder rent praktisk, at hvis en normal husholdning har 10 enheder forbundet til internettet, så er 3 måske 4 af dem en IoT-enhed. I takt med at der kommer flere og flere IoT-enheder i hjemmet viser statistikken at der i år 2025 vil være samlet 75.44 milliarder enheder forbundet til internettet [4].
Paloalto frigav en rapport tilbage i år 2020 som viste, at over 50% af alle IoT-enheder havde en sårbarhed som blev rangeret fra medium til høj. Bliver der kigget på matematikken giver dette 37.72 milliarder enheder som potentielt har en medium til høj sårbarhed. [9]

Artiklen fokuserer hovedsageligt på fire metoder til at finde sårbarheder i den firmware, som IoT-enheder bliver solgt med. Her nævnes fire metoder som er emulator baseret tests, automatisk kode analyse, netværks test og manuel reverse engineering. Til fælles har metoderne et højt tekniske niveau, ikke et niveau som den normale forbruger kan forventes at besidde. Dette er også en tidskrævende proces, og forudsætter at fabrikanterne samarbejder mht. at dele deres firmware. Til trods for at der bliver brugt meget tid på at teste IoT-enheders firmware hos forskere og sårbarhedstestere er det stadigvæk en svær og tung proces. [9]
Derudover bliver der lagt vægt på vigtigheden af at fabrikanter får implementeret seriøse og grundige sikkerheds test så udbredelsen af sårbare IoT-enheder mindskes så meget som muligt. Metoden til at finde sårbarheder i IoT-enheder er svært og kræver stor teknisk forståelse og indsigt. [9]

Hovedbudskabet i artiklen er, at det er af afgørende betydning at have en stærk sikkerhedsproces for IoT-enheder, som inkluderer en pålidelig metode til at opdage og finde sårbarheder i firmware. Der er flere teknikker og tilgange til at finde sårbarheder, men det er vigtigt at vælge den mest hensigtsmæssige til den specifikke situation, og tage højde for de begrænsninger, der er forbundet med at teste IoT-enheder. Artiklen understreger også vigtigheden af yderligere forskning på området, for at udvikle mere effektive metoder til at opdage og afhjælpe sårbarheder i IoT-enheder. Det er vigtigt at teste firmware på IoT-enheder for at opdage og rette sårbarheder, da disse enheder typisk har begrænsede ressourcer og kan være sårbare over for cyberangreb. Uden grundig firmware-testning kan sårbarheder i enhederne udnyttes af angribere, hvilket kan føre til tab af data og skade på enheder og infrastruktur. [9]

### 4.4.2 REVIEW AF (NR. 2): VULNERABILITY STUDIES AND SECURITY POSTURES OF IOT DEVICES: A SMART HOME CASE STUDY

Artiklen præsenterer en undersøgelse af sikkerhedstrusler og sårbarheder i smart home-enheder, herunder smarte lyspærer, termostater, dørlåse og overvågningskameraer. Forskerne identificerede sårbarheder, der kan udnyttes af angribere til at få adgang til og kontrollere disse enheder. Artiklen fremhæver vigtigheden af at beskytte IoT-enheder mod trusler og sårbarheder for at undgå cyberangreb og dets potentielle konsekvenser. [10]

Artiklen beskriver en undersøgelse af sårbarheder i forskellige typer IoT-enheder og kommer med anbefalinger til at forbedre deres sikkerhed. Forskerne har gennemført en litteraturgennemgang og en række eksperimenter på forskellige typer IoT-enheder herunder smart home-enheder såsom smartpærer, smart termostater og smarte kameraer.
Eksperimenterne blev udført for at teste enhedernes sikkerhed mod forskellige typer angreb, herunder fysiske angreb, netværksangreb, softwareangreb og krypteringsangreb. I artiklen blev der udført flere typer angreb på de undersøgte IoT-enheder, herunder fysiske angreb (såsom at knække en pære for at få adgang til dens kredsløb), netværksangreb (som man-in-the-middle-angreb og DoS-angreb), softwareangreb (såsom at udnytte sårbarheder i firmware eller angribe en enhed via en sårbar mobilapp) og krypteringsangreb (som at dekryptere en enheds netværkstrafik eller brute-force-adgangskoder).
De udførte også reverse engineering på enhederne for at undersøge deres firmware og firmware-opdateringer.
Forskerne konkluderede, at kendte og populære IoT-enheder fra kendte producenter har en stærkere sikkerhedsprofil end mindre kendte enheder fra mindre kendte producenter. De påpegede også, at undersøgelser af sårbarheder i IoT-enheder har tendens til at fokusere på kendte enheder og producenter, mens mindre kendte enheder og producenter bliver overset. Forskerne opfordrede til, at der skal foretages flere undersøgelser af sårbarheder i IoT-enheder fra mindre kendte producenter. De anbefalede også, at standarder for sikkerheds- og funktionskrav for IoT-enheder skal standardiseres for at øge deres sikkerhed. [10]

Desuden kan resultaterne af disse undersøgelser også bruges til at udvikle nye standarder og ”best practices”[1] for sikkerhed i IoT-enheder, hvilket kan hjælpe producenterne med at implementere sikkerhedsforanstaltninger tidligt i designfasen. Dette kan også give forbrugere større tillid til IoT-enheder og øge deres accept af teknologien.
Samlet set kan brugen af disse metoder bidrage til at styrke IoT-enheder mod cyberangreb og øge deres pålidelighed og sikkerhed i hjemmet.

Sikkerhedsrisici i IoT-enheder udgør en øget trussel mod privatliv og sikkerhed, og dette studie understreger behovet for at forbedre sikkerheden i disse enheder. Ved at anvende systematiske undersøgelsesmetoder og best practices, som beskrevet i artiklen, kan producenter og brugere styrke IoT-enheder mod cyberangreb og forbedre deres pålidelighed og sikkerhed. Det er afgørende, at der tages handling for at sikre IoT-enheder mod potentielle trusler og sikre et sikkert og tillidsfuldt digitalt miljø.

[1] ”best practices” refererer til de metoder, procedurer og standarder, som er anerkendt som værende mest effektive og sikre i en given situation eller i en given branche.

### 4.4.3 REVIEW AF (NR. 3): A LARGE-SCALE EMPIRICAL STUDY ON THE VULNERABILITY OF DEPLOYED IOT DEVICES

Artiklen handler om en stor empirisk undersøgelse af sårbarheder i Internet of Things (IoT) enheder, som er blevet udrullet i virkelige miljøer. Forfatterne af artiklen har gennemført en 10 måneders undersøgelse af 1,362,906 IoT-enheder og fundet ud af, at N-Days[2] sårbarhedsangreb stadig er en alvorlig trussel for IoT-enheder og kræver øjeblikkelig opmærksomhed. Artiklen fremhæver også forskelle i IoT-søgemaskiner og de begrænsninger, der er forbundet med leverandørernes forsvar mod disse angreb. [11]

For at opnå deres resultater har forfatterne udført en empirisk undersøgelse af 1.362.906 IoT-enheder, der var i brug over en periode på ti måneder. I deres undersøgelse har forfatterne anvendt en kombination af metoder, der inkluderer firmware-fingerprinting til at identificere N-Days sårbarheder i de testede IoT-enheder og IoT-søgemaskiner som Shodan, Censys, BinaryEdge, ZoomEye og GreyNoise til at identificere og samle data om de testede IoT-enheder.
Firmware-fingerprinting-metoden involverer en undersøgelse af de enkelte IoT-enheder for at identificere og validere, om firmware-versionen på enheden indeholder en kendt sårbarhed. Metoden kræver ikke ejerskab af enheden og udnytter ikke sårbarhederne, så den anses for at være en acceptabel og etisk metode til at teste online-enheder.
For at indsamle data om de testede IoT-enheder har forfatterne brugt IoT-søgemaskiner, der er almindeligt anvendt til at indsamle data om IoT-enheder på internettet. Ved at analysere resultaterne fra de forskellige IoT-søgemaskiner, har forfatterne kunnet evaluere og sammenligne søgemaskinernes præcision og dækkeevne.
Desuden har forfatterne også analyseret MQTT-servere, som millioner af IoT-enheder kommunikerer med, og de har identificeret 64.309 live MQTT-servere, hvoraf mange er udsat for alvorlige sikkerhedstrusler på grund af manglende adgangskodebeskyttelse. For at indsamle data om MQTT-serverne har forfatterne anvendt både IP-range information fra populære Cloud Service Platforms som Amazon Web Services (AWS), Google Cloud og Microsoft Azure og søgemaskiner som Shodan.
I deres undersøgelse har forfatterne også sammenlignet og evalueret forsvarsmekanismer fra forskellige IoT-enhedsproducenter mod N-Days sårbarheder og konstateret begrænsninger og mangler i de nuværende forsvarsmekanismer.
På trods af deres store empiriske undersøgelse, påpeger forfatterne nogle begrænsninger i deres metoder, som kan føre til falske positive resultater. For eksempel kan deres firmware-fingerprinting-metode være begrænset af nøjagtigheden af den kendte sårbarhed og dens tilhørende firmware-version [11].

De vigtigste takeaways fra artiklen er, at N-Days sårbarheder stadig er en betydelig trussel mod IoT-enheder, og at dette problem kræver mere opmærksomhed og forbedring fra producenterne af IoT-enheder. Der er en betydelig mængde IoT-enheder, som stadig er sårbare over for disse angreb. Artiklen viser, at der stadig er et stort antal IoT-enheder, der mangler grundlæggende sikkerhedsforanstaltninger og password beskyttelse, hvilket gør dem sårbare over for angreb fra hackere. Desuden viser artiklen også forskelle blandt de fem IoT søgemaskiner, som blev undersøgt i denne undersøgelse. Endelig er det vigtigt at bemærke, at der stadig er et stort behov for mere effektive modforanstaltninger til at beskytte IoT-enheder mod sikkerhedstrusler.

[2] En n-dages sårbarhed er en sikkerhedsrisiko i computersoftware, hvor producenten er opmærksom på sårbarheden og måske allerede har udstedt (eller er i gang med at arbejde på) en rettelse eller en løsning. Der findes ofte allerede aktive exploits af sårbarheden, som venter på at blive misbrugt af ondsindede aktører.

### 4.4.4 REVIEW AF (NR. 4): VULNERABILITIES AND SECURITY ISSUES IN IOT PROTOCOLS

Artiklen diskuterer de vigtigste protokoller, der anvendes i IoT-netværk hvor deres funktioner og sikkerhedsproblemer bliver analyseret. For eksempel påpeges det, at en af de store udfordringer for IoT-protokoller er at sikre datafortrolighed og forhindre uautoriseret adgang til enheder og data. Artiklen diskuterer også metoder og løsninger på disse problemer og foreslår, hvordan protokoller som DDS, MQTT og LoRaWAN kan forbedres. Endelig præsenterer artiklen en sammenligning af de tre protokoller baseret på deres transportlag, arkitektur, sikkerhedsegenskaber og de væsentligste sikkerhedsproblemer. [12]

For at evaluere sikkerheden ved disse protokoller blev der udført en omfattende litteraturgennemgang og analyse af tilgængelige sikkerhedsprotokoller, og forskellige sårbarheder og angrebsformer blev identificeret. Artiklen beskriver også potentielle løsninger og forbedringer, der kan implementeres for at styrke sikkerheden i de pågældende protokoller.
For DDS blev sikkerhedsproblemerne identificeret gennem en undersøgelse af dens publish-subscribe model, QoS-politikker og miljøvariabler. Flere løsninger blev foreslået for at styrke DDS-sikkerheden, inklusive DDS Security Standard 1.0, Connext DDS Secure og OpenDDS-systemet.
For MQTT fandt forfatterne, at det var sårbart over for DoS-angreb, og at miljøvariabler kunne ændres, hvilket kunne føre til sikkerhedssvagheder. For at løse disse problemer blev der foreslået forskellige løsninger, herunder session keys, throttling og Secure-MQTT.
LoRaWAN blev identificeret som sårbart over for eksponering af nøgler og manglende evne til at give en sikker end-to-end-forbindelse. Der blev identificeret flere sårbarheder, herunder replay-angreb på ABP-aktiverede noder, bit-flipping-angreb, overvågning, ACK-spoofing og LoRa-klasse B-angreb. [12]

Artiklen præsenterer en gennemgang af tre populære IoT-protokoller (DDS, MQTT og LoRaWAN) og de sikkerhedsmæssige udfordringer, de kan have. En vigtig anbefaling er at forbedre sikkerheden i disse protokoller ved at implementere løsninger som session keys, throttling og Intrusion Detection systems, samt at re-key[3] ofte og reducere brugen af aktivering efter konfiguration[4]. Det er også vigtigt at indføre en kryptografisk beskyttet pseudo-tilfældig nummergenerator og fysisk sikring af enhederne for at forhindre uautoriseret adgang.

[3] Re-key betyder at generere en ny nøgle til kryptering af data. Teknikken bruges til at forhindre, at en angriber kan få adgang til tidligere krypterede data, hvis den oprindelige nøgle er blevet kompromitteret.
[4] Det indebærer, at det er anbefalet at minimere brugen af en proces kaldet "activation" efter konfiguration af en enhed, da denne handling kan gøre enheden mere sårbar over for sikkerhedsangreb.

### 4.4.5 REVIEW AF (NR. 5): IOT NETWORKS: SECURITY VULNERABILITIES OF APPLICATION LAYER PROTOCOLS

Artiklen handler om de sikkerhedsmæssige udfordringer forbundet med IoT-applikationslagprotokoller. Protokoller som CoAP, AMQP, DDS, XMPP og MQTT anvendes i IoT-netværk og er ansvarlige for at overføre data fra IoT-enheder til slutbrugere. Artiklen gennemgår de mest almindelige sårbarheder, der findes i disse protokoller og beskriver, hvordan de kan udnyttes af ondsindede aktører. Desuden giver artiklen også en beskrivelse af de eksisterende sikkerhedsforanstaltninger og fremtidsperspektiverne for at sikre IoT-applikationslagprotokoller. [13]

For at komme frem til deres resultater, har forfatterne gennemgået en omfattende undersøgelse af fire forskellige IoT-applikationslagprotokoller: CoAP, AMQP, DDS og MQTT. For hver protokol har de identificeret potentielle sikkerhedstrusler og sårbarheder og undersøgt, hvordan protokollernes sikkerhedsmekanismer beskytter mod disse trusler. De har også undersøgt, hvor effektive protokollernes sikkerhedsmekanismer er i praksis ved at analysere data fra National Vulnerability Database (NVD) fra de sidste seks år.
For at identificere sikkerhedstruslerne har forfatterne gennemgået de fire protokollers specifikationer og dokumentation og har analyseret de potentielle svagheder i deres sikkerhedsprotokoller. De har også undersøgt og analyseret de sikkerhedstrusler, der er blevet rapporteret i NVD i løbet af de sidste seks år. Gennem denne undersøgelse har forfatterne været i stand til at identificere de mest almindelige sikkerhedstrusler for hver protokol og evaluere effektiviteten af deres sikkerhedsprotokoller i praksis. Disse sikkerhedstrusler/angreb inkluderer blandt andet Man-in-the-Middle angreb, hvor en hacker kan aflytte og ændre kommunikationen mellem IoT-enheder og deres servere. Derudover kan der ske angreb på selve autentificerings- og autorisationsprocessen, hvilket kan give hackere adgang til fortrolige data og systemer. Endelig kan der opstå problemer med håndteringen af messages og caching, hvilket kan åbne op for sårbarheder og DDoS-angreb. [13]

Det er bekymrende at artiklen viser, at selv de mest udbredte IoT-protokoller er sårbare over for forskellige former for angreb og sårbarheder. Det viser, hvor vigtigt det er for udviklere af IoT-enheder og -protokoller at have en klar og grundig tilgang til sikkerhed og privathed, når de udvikler deres produkter. Det er også vigtigt, at virksomheder og organisationer, der bruger IoT-enheder og -protokoller, har en klar forståelse af, hvad deres enheder gør, og hvordan de er sikret. Disse trusler skal tages alvorligt og der skal ligeledes arbejdes hen imod mere sikre og pålidelige IoT-protokoller, der kan beskytte data og brugerprivathed.

### 4.4.6 REVIEW AF (NR. 6): A SURVEY ON THE SECURITY VULNERABILITIES OF IOT SMART HOME APPLICATION

Artiklen diskuterer sårbarhederne i IoT-enheder i Smart Home-applikationer. De mest almindelige sårbare punkter er adgangskontrol, godkendelse og kryptering. Adgangskontrol er især vigtig, da det kan føre til uautoriseret adgang og manipulation af data. Der er også risiko for datalækager, hvor IP-adresser og pakkestørrelser kan afsløre personlige oplysninger. Godkendelse er også et centralt område, da det kan føre til uautoriseret adgang, hvis adgangskoder eller fingeraftryk bliver stjålet. Kryptering er også afgørende for at beskytte fortroligheden af data, og mange angreb sigter mod at afsløre krypteringsmetoderne. [14]

Forskerne udførte en systematisk litteraturundersøgelse ved at identificere relevante artikler ved hjælp af nøgleord som "IoT security", "Smart Home security", "IoT authentication" og "IoT Access Control". Forskerne identificerede manglende authentication, adgangskontrol og sikker kommunikation som de største sikkerhedsproblemer i IoT Smart Home-applikationer. De fremhæver også behovet for at udvikle en multi-layered sikkerhedsramme, der kan håndtere sikkerhedsproblemer i alle lag i IoT-arkitekturen. En multi-layered sikkerhedsramme betyder, at der er implementeret flere sikkerhedsforanstaltninger på forskellige lag i IoT-arkitekturen for at øge beskyttelsen mod sikkerhedstrusler. Dette indebærer en sikkerhedsløsning, der ikke kun adresserer sikkerhed på enhedsniveau, men også tager hensyn til sikkerhed i andre lag, såsom controller, netværk og cloud. En multi-layered sikkerhedsramme kan give en mere omfattende og integreret tilgang til sikkerhed, som gør det mere effektivt at beskytte IoT-enheder. Ved at benytte en systematisk og objektiv tilgang til undersøgelsen, kunne forskerne minimere bias og sikre, at alle relevante artikler blev inkluderet.
Derudover fandt de, at eksisterende tilgange til at håndtere sikkerhedsproblemer i IoT Smart Home-applikationer ofte var begrænset til at adressere problemer på enhedsniveau, og ikke på controller- eller cloud-lagene. [14]

Det er alarmerende, at der stadig er så mange sikkerhedshuller i IoT-enheder, da det er en teknologi, der bliver mere og mere udbredt i hjem over hele verden. Det er vigtigt at tage sikkerheden alvorligt i design og implementering af disse for at beskytte både brugerne og deres data. Samlet set viser artiklen, at der stadig er et stort potentiale for at forbedre sikkerheden i IoT-enheder, og at der er behov for en øget fokus på at adressere sårbarheder.

### 4.4.7 REVIEW AF (NR. 7): INTERNET OF THINGS (IOT): VULNERABILITIES, SECURITY CONCERNS AND THINGS TO CONSIDER

Artiklen handler om de sikkerhedsmæssige udfordringer ved IoT-enheder teknologien, som er en teknologi, der forbinder fysiske enheder til internettet og giver dem evnen til at samarbejde og indsamle data. Artiklen identificerer og diskuterer de mest almindelige trusler og sårbarheder, der findes i IoT-systemer og foreslår potentielle løsninger på disse sikkerhedsproblemer. [15]

For at undersøge de sikkerhedsmæssige udfordringer ved IoT-enheder, har forskerne gennemgået en række tidligere studier og artikler om emnet. De har derefter analyseret de forskellige trusler og sårbarheder, der er blevet beskrevet i disse kilder og udarbejdet en oversigt over de vigtigste sikkerhedsproblemer. Forskerne har også undersøgt den grundlæggende arkitektur af IoT og identificeret de sikkerhedsrisici, der kan opstå på hver enkelt lag i protokolstakken. Desuden har de udforsket forskellige løsninger og metoder, der kan anvendes til at forbedre sikkerheden i IoT, og vurderet deres potentiale til at håndtere de identificerede trusler. Forskerne foreslår at forbedre datakryptering og autentificering, udvikle mere robuste sikkerhedsalgoritmer og standardisere IoT-udviklingsplatforme. Der foreslås en forbedring af det eksisterende multi-lags IoT-arkitektur med fokus på sikkerheden i interface, transmissionssikkerhed, fysisk sikkerhed og datakrypteringsmetoder. Derudover skal der udvikles en fælles standard for udvikling af IoT-platforme, da der i øjeblikket ikke er nogen på markedet. Algoritmerne for IoT-enheder skal også undersøges grundigt for at identificere eventuelle sårbarheder eller begrænsninger, der kan føre til datalækager eller -tyveri. Endelig foreslår forskerne at studere sikkerhedsteknologier som blockchain og vurdere deres anvendelse i eksisterende IoT-frameworks for at gøre dem mere sikre i forhold til dataoverførsel og dataautenticitet. Alle disse foranstaltninger skal testes i realtid for at sikre deres effektivitet, og det kræver en langsigtet investering i IoT-sikkerhed og -standardisering. [15]

Artiklen giver en god oversigt over vigtige sikkerhedsrisici, som IoT-enheder er udsat for. Den fremhæver forskellige former for angreb, herunder Denial of Service (DoS), man-in-the-middle (MitM) og SCADA-angreb. Der fremhæves også andre alvorlige sikkerhedsproblemer såsom data og identitetstyveri, mangelfuld software/firmware sikkerhed og fysiske sikkerhedsrisici. Forskerne foreslår forskellige foranstaltninger for at sikre IoT-enhederne, herunder en forbedring af den eksisterende IoT-arkitektur, mere robuste IoT-sikkerhedsalgoritmer og anvendelse af blockchain teknologi. Selvom artiklen giver en grundig oversigt over IoT-sikkerhedsrisici og foreslår flere interessante foranstaltninger til at forbedre sikkerheden, er det vigtigt at bemærke, at implementering af disse foranstaltninger kan være komplekst og kræver yderligere forskning og udvikling.

### 4.4.8 REVIEW AF (NR. 8): VULNERABILITY CLASSIFICATION OF CONSUMER-BASED IOT SOFTWARE

Artiklen præsenterer en kategorisering af sårbarheder i SmartThings-platformen, som er en af de største smart home-platforme. Forskerne bag artiklen har undersøgt og identificeret forskellige sårbarheder i SmartThings-platformen og har klassificeret dem ved hjælp af et framework, der tager højde for angrebsmetoder, platformkomponenter og tilhørende afhjælpninger. Artiklens formål er at give udviklere og sikkerhedseksperter et bedre overblik over sårbarhederne i SmartThings-platformen samt strategier for bedst mulig beskyttelse mod disse. SmartThings er en platform til smart home automation, der blev grundlagt i 2012 og opkøbt af Samsung. Det giver mulighed for integration af forskellige IoT-enheder til det smarte hjem. Det har en hub-enhed, en app og et cloudbaseret kontrolpanel, der giver brugerne mulighed for at overvåge og styre deres smart home-enheder centralt. SmartThings kan integreres med andre IoT-platforme og -enheder, og er en af de mest alsidige og populære smart home-platforme. [16]

I artiklen undersøges sårbarhederne i SmartThings-platformen. For at analysere sårbarhederne anvendes Neshenko framework til sårbarhedskategorisering, som tilpasses til SmartThings-platformen og linkes til OWASP's Top-10 og MITRE ATT&CK. Forskerne gennemgår SmartThings-platformens komponenter og identificerer forskellige sårbarheder, herunder SQL-injektion, bufferoverløb, uautoriseret adgang, URL-injektion, Integer-underflow[5] og dataoverførselsangreb. Ved at anvende frameworket kunne forskerne kategorisere sårbarhederne og foreslå passende mitigationsteknikker for hver kategori.
Forskerne foreslår at neutralisere argumentdelimitorer[6] for at afhjælpe sårbarheden ved URL-injektion og anbefaler at verificere længden af JSON-værdier for at undgå bufferoverløb. Desuden anbefaler forskerne applikationsvurderingsteknikker for at sikre, at apps ikke udnytter sårbarhederne. For at afhjælpe sårbarheden for uautoriseret adgang til enheder anbefales det, at der anvendes adgangskontrol og autentificeringsprotokoller.
Undersøgelsen af SmartThings-platformens sårbarheder og den anvendte metode kan give en forståelse af, hvordan IoT-platforme kan analyseres for sårbarheder. Artiklen giver også et overblik over de vigtigste sårbarheder og foreslår relevante mitigationsteknikker til at minimere risikoen for sikkerhedsbrud i SmartThings-platformen. [16]

Artiklen fremhæver behovet for at uddanne udviklere om sikkerhed, da mange sårbarheder skyldes fejl i koden eller dårlige programmeringspraksis. Det er vigtigt, at udviklere har et godt kendskab til de bedste sikkerhedspraksis og er i stand til at identificere og afhjælpe potentielle sårbarheder.
Samlet set er artiklen en vigtig påmindelse om behovet for sikkerhed i IoT-systemer som SmartThings og understreger vigtigheden af at have en omfattende tilgang til sikkerhed, der dækker hele systemets livscyklus.

[5] "Integer underflow" betyder på dansk "heltalsunderflow". Det sker, når et heltal bliver reduceret til et negativt tal, når det bliver trukket fra et andet heltal, som er større end det første. Det kan føre til unødvendige fejl eller sårbarheder i software.
[6] Argumentdelimitorer er tegn eller symboler, der adskiller forskellige argumenter i en kommando eller en besked. De bruges til at identificere, hvor et argument starter og slutter. Hvis disse tegn ikke behandles korrekt, kan de udnyttes af en angriber til at indsætte ondsindet kode eller få adgang til systemressourcer, som de ikke burde have adgang til.

## 4.5 KONKLUSION AF RESULTATERNE FRA REVIEWS

Internet of Things (IoT) er en stadig mere udbredt teknologi, der forbinder fysiske enheder til internettet og gør dem i stand til at samarbejde og indsamle data. Som med alle teknologier er der også potentielle sikkerhedsmæssige udfordringer forbundet med IoT-enheder og -systemer, og dette emne har været i fokus for forskning i de seneste år. Denne delkonklusion vil diskutere de vigtigste konklusioner, der kan drages fra de 8 artikler gennemgået i denne review.

**Sikkerhedsproblemer i IoT-enheder**
En af de vigtigste konklusioner fra artiklerne er, at der stadig er en række sikkerhedsproblemer i IoT-enheder og -systemer, der skal håndteres. Dette omfatter blandt andet manglende autentificering og adgangskontrol, usikker kryptering, sårbarheder i hardware og software, angreb på controller- og cloud-lagene og fysiske sikkerhedsrisici. Flere af artiklerne fremhæver også behovet for at udvikle en mere omfattende og integreret tilgang til sikkerhed, der dækker hele IoT-systemets livscyklus.

**IoT-arkitektur og sikkerhed**
Artiklerne viser, at IoT-arkitekturen spiller en vigtig rolle i sikkerheden af IoT-enheder og -systemer. Flere af artiklerne foreslår at forbedre eksisterende IoT-arkitekturer for at adressere de sikkerhedsmæssige udfordringer på alle lag af protokolstakken. Dette indebærer implementering af flere sikkerhedsforanstaltninger på forskellige lag i IoT-arkitekturen for at øge beskyttelsen mod sikkerhedstrusler. En multi-layered sikkerhedsramme kan give en mere omfattende og integreret tilgang til sikkerhed, som gør det mere effektivt at beskytte IoT-enheder.

**Standardisering af IoT-enheder**
Standardisering af IoT-enheder er også et vigtigt emne, som flere af artiklerne diskuterer. Da der ikke er nogen standardiseret tilgang til IoT-udvikling, kan dette føre til manglende sikkerhed og interoperabilitet mellem forskellige IoT-enheder og -systemer. Flere artikler fremhæver behovet for at standardisere IoT-udviklingsplatforme og algoritmer for at forbedre sikkerheden og interoperabiliteten af IoT-enheder.

**Uddannelse og bevidsthed om sikkerhed**
En anden vigtig konklusion fra artiklerne er, at uddannelse og bevidsthed om sikkerhed er afgørende for at forbedre sikkerheden i IoT-enheder og -systemer. Udviklere skal have et godt kendskab til de bedste sikkerhedspraksis og være i stand til at identificere og afhjælpe potentielle sårbarheder.

Desuden er det vigtigt at øge bevidstheden om IoT-sikkerhed blandt brugere og virksomheder, da de spiller en afgørende rolle i at beskytte deres data og enheder. Brugere skal instrueres i at vælge pålidelige enheder, ændre standardadgangskoder og sikre, at enhederne er opdaterede med den nyeste sikkerhedssoftware. Virksomheder skal prioritere IoT-sikkerhed og inkorporere sikkerhedsfunktioner i deres produkter fra starten af udviklingscyklussen.
En anden vigtig faktor i at sikre IoT-enheder er standardisering. Der er behov for en global standard for IoT-sikkerhed for at sikre, at alle enheder overholder en minimumsstandard og forbedrer interoperabiliteten mellem enhederne. Standardiseringen bør omfatte sikkerhed på tværs af enheder, kommunikationsprotokoller og sikkerhedsforanstaltninger på controller- og cloud-niveau.

Blockchain-teknologi kan også være en løsning på nogle IoT-sikkerhedsproblemer. Blockchain kan sikre, at dataoverførsler er autentiske, sikre og ikke kan manipuleres af angribere. Denne teknologi kan også hjælpe med at decentralisere IoT-enheder, så de er mere modstandsdygtige over for angreb.

Endelig er det afgørende at foretage yderligere forskning og udvikling af IoT-sikkerhedsforanstaltninger. Forskere og udviklere skal arbejde sammen for at undersøge og afhjælpe eksisterende sårbarheder og udvikle nye sikkerhedsfunktioner og -protokoller. Det kræver en langsigtet investering i IoT-sikkerhed og standardisering for at sikre, at enhederne forbliver sikre i fremtiden.

I konklusionen kan det fastslås, at IoT-teknologien har potentiale til at revolutionere måden, vi interagerer med vores omgivelser på, men det er også en teknologi, der er sårbar over for sikkerhedstrusler og angreb. Det er vigtigt at tage IoT-sikkerhed alvorligt, og alle parter, herunder udviklere, producenter, virksomheder og brugere, har et ansvar for at beskytte enhederne og dataene. Gennem standardisering, blockchain-teknologi, uddannelse og forskning kan vi forbedre sikkerheden i IoT-enheder og sikre, at denne teknologi kan bruges sikkert og effektivt i fremtiden.

# 5 SIKKERHEDSTILTAG I HJEMMET

IT-sikkerhed i hjemmet er vigtig, da stadig flere enheder og systemer er forbundet til internettet. Det er afgørende at have en forståelse af de risici, der er forbundet med IT-sikkerhed i hjemmet, og hvordan trusler kan forebygges ved hjælp af almindelige sikkerhedstiltag. Det er også vigtigt at være opmærksom på udfordringerne i forbindelse med brug af IoT-enheder i hjemmet og hvordan ISO 27001 sikkerhedsledelse kan implementeres til bedre IT-sikkerhed.

Dette afsnit dækker flere emner i forbindelse med IT-sikkerhed i hjemmet. Der tages højde for risikofaktorerne forbundet med IT-sikkerhed i hjemmet, de normale sikkerhedstiltag, som kan forebygge IT-relaterede trusler, og de sikkerhedsudfordringer, der kan være forbundet med IoT-enheder. Der diskuteres også betydningen af bevidsthed og uddannelse i hjemmet om IT-sikkerhed og hvordan dette kan bidrage til et mere sikkert hjemmemiljø. Der gives også gode råd til IT-sikkerhed i hjemmet fra flere kilder, og der diskuteres fremtidsperspektiverne for IT-sikkerhed i hjemmet.

Her ses en oversigt over dette afsnits emner:

**Introduktion**: I introduktionen gives en definition af, hvad hjemmesikkerhed er, og hvorfor det er vigtigt at have fokus på IT-sikkerhed i hjemmet. Derudover beskrives forskellige standarder og rammer for IT-sikkerhed i hjemmet.

**Risikofaktorer for IT-sikkerhed i hjemmet**: Her beskrives de forskellige risikofaktorer, der kan påvirke IT-sikkerheden i hjemmet, herunder sårbare enheder og systemer samt sårbar brugeradfærd.

**Normale sikkerhedsforanstaltninger for at forebygge IT-relaterede trusler**: I dette afsnit beskrives forskellige sikkerhedsforanstaltninger, som kan hjælpe med at forebygge IT-relaterede trusler i hjemmet. Dette inkluderer bl.a. opdatering af software og enheder, brug af stærke passwords og to-faktor-autentifikation, VPN og kryptering af netværk.

**IoT-enheder i hjemmet og dets sikkerhedsudfordringer**: Her beskrives, hvad IoT-enheder er, og hvordan de fungerer i hjemmet. Derudover beskrives forskellige sikkerhedsudfordringer, som kan påvirke IoT-sikkerheden, herunder hacking, datamisbrug og sikkerhedsbrister i enheder. Endelig beskrives forskellige sikkerhedstiltag, der kan hjælpe med at beskytte IoT-enheder.

**ISO 27001 og sikkerhedsledelse i hjemmet**: I dette afsnit beskrives, hvad ISO 27001 er, og hvordan det kan anvendes i forhold til IT-sikkerhed i hjemmet. Derudover beskrives fordele og ulemper ved implementering af ISO 27001 i hjemmet samt udfordringerne ved dens implementering og strategier for håndtering af disse udfordringer.

**Implementering af ISO 27001 i hjemmet**: Her beskrives de forskellige krav for at implementere ISO 27001 i hjemmet, herunder risikovurdering og risikohåndtering i forhold til IT-sikkerhed i hjemmet samt sikkerhedsstyring og dokumentation af sikkerhedsprocedurer i hjemmet.

**Bevidsthed og uddannelse om ISO 27001 i hjemmet**: I dette afsnit beskrives, hvorfor det er vigtigt at have bevidsthed og uddannelse om ISO 27001 og IT-sikkerhed i hjemmet. Derudover beskrives forskellige måder, hvorpå uddanne kan oplyse familien om ISO 27001 og IT-sikkerhed.

**Fremtidsudsigter for IT-sikkerhed og ISO 27001 i hjemmet**: Her diskuteres, hvordan IT-sikkerhed og ISO 27001 kan udvikle sig i fremtiden, samt hvordan ISO 27001 kan tilpasses og sikkerhedsprocedurer i hjemmet til nye teknologier og trends.

**Udvikling af en minificeret version af ISO 27001 til hjemmet**: I dette afsnit beskrives, hvordan en simplificeret version af ISO 27001 kan udvikles, der er tilpasset til IT-sikkerheden i hjemmet. Dette inkluderer at identificere IT-sikkerhedstrusler og sårbarheder i hjemmet, udvikling af IT-sikkerhedspolitik og procedurer for hjemmet, implementering af sikkerhedsstyring i hjemmet, uddannelse og opbygning af bevidsthed om IT-sikkerhed i hjemmet samt opfølgning på sikkerhedsprocedurer og retningslinjer for IT-sikkerhed i hjemmet.

**Hvad er mest realistisk at forvente ift. hjemmesikkerheden:** I dette afsnit beskrives, hvordan den generelle forventning kan være ift. hjemmesikkerheden.

**De 7 gode råd til IT-sikkerhed fra sikkerdigital.dk**: I dette afsnit præsenteres 7 gode råd til IT-sikkerhed i hjemmet fra sikkerdigital.dk, herunder at holde software og enheder opdateret, bruge stærke passwords og to-faktor-autentifikation, være opmærksom på phishing og andre råd.

**De 10 gode råd til IT-sikkerhed fra Dubex og CSIS**: Her præsenteres 10 gode råd til IT-sikkerhed i hjemmet fra Dubex og CSIS, herunder at have en ledelse, segmentere adgang, sikre leverandører og andre råd.

## 5.1 INTRODUKTION

Sikkerhed i hjemmet, særligt inden for informationsteknologi, er blevet en uomgængelig del af hverdagen i den digitale tidsalder. Beskyttelse af personlige enheder og data mod online trusler kræver ikke bare passende sikkerhedsforanstaltninger, men også bevidsthed om sikker online opførsel. Med fremkomsten af IoT-enheder bliver sikkerhedstiltag stadig mere vigtige, da flere og flere enheder bliver forbundet og dermed potentielt sårbare. Dette udstikker vigtigheden af at forstå og implementere relevante IT-sikkerhedsrammer og standarder. Selvom der findes et antal etablerede standarder, som ISO 27001 [17], NIST Cybersecurity Framework [18] og ENISA Cybersecurity Guidelines [19], kan kompleksiteten i disse modeller kræve alternative, simplificerede tilgange til hjemmebrug for at fremme en bredere forståelse og bevidsthed om IT-sikkerhed i hjemmet.

### 5.1.1 HVAD ER SIKKERHED I HJEMMET

Hjemme-IT-sikkerhed omhandler beskyttelse af personlige enheder, data og oplysninger mod internetbaserede trusler og angreb. Det er vigtigt at have passende sikkerhedsforanstaltninger, som stærke adgangskoder og regelmæssige softwareopdateringer, samt at undgå at dele personlige oplysninger og besøge usikre websider. Det er essentielt at lære børn om betydningen af IT-sikkerhed og træffe kloge valg online.

### 5.1.2 VIGTIGHEDEN AF SIKKERHEDSTILTAG I HJEMMET

Sikkerhedstiltag er afgørende for IT og IoT-enheder i hjemmet, da vores enheder og oplysninger er forbundet til internettet og dermed sårbare over for cyberangreb. Ved at tage passende forholdsregler kan vi beskytte vores enheder og oplysninger og bevare vores personlige oplysningers privatliv.

### 5.1.3 RAMMEVÆRK OG STANDARDER INDEN FOR IT-SIKKERHED TIL HJEMMET

Flere rammeværk og standarder kan hjælpe med hjemme-IT-sikkerhed, såsom ISO 27001 [17], NIST Cybersecurity Framework [18] og ENISA Cybersecurity Guidelines [19]. Disse standarder giver retningslinjer for at forbedre IT-sikkerheden på en systematisk måde.

Alle tre standarder fokuserer på at skabe en formel tilgang til IT-sikkerhed og hjælpe med at identificere risici, trusler og passende sikkerhedsforanstaltninger. Dog kan deres kompleksitet gøre det vanskeligt at implementere dem direkte i hjemmet. Derfor er der behov for at overveje alternative tilgange, som en simplificeret version af standarderne, der kan anvendes i hjemmemiljøet. Dette vil bidrage til at øge bevidstheden og forståelsen af IT-sikkerhed i hjemmet.

## 5.2 RISIKOFAKTORER FOR IT-SIKKERHED I HJEMMET

Hjemmets IT-sikkerhed omfatter enheder som routere, computere, smart home-enheder og Wi-Fi Access Points, alle er potentielt udsatte for cyberangreb med konsekvenser som identitetstyveri og datatab. Passende sikkerhedsforanstaltninger, herunder stærke adgangskoder, opdateret firmware og robust kryptering, er essentielle. Brugeradfærd, herunder brug af svage passwords og data deling, kan øge sårbarheden. Derfor er det afgørende at uddanne brugere i sikker online adfærd.

### 5.2.1 UDSATTE ENHEDER OG SYSTEMER

Routere er en central del af ethvert hjemme-netværk, da de styrer trafikken mellem internettet og de forskellige enheder i hjemmet. Desværre er routere også en af de mest udsatte enheder, da de kan blive kompromitteret af angribere, der ønsker at få adgang til hjemmenetværket. Dette kan føre til et hav af alvorlige problemer, såsom identitetstyveri, datatab og økonomisk svindel. Derfor er det vigtigt at sikre, at routeren har en stærk adgangskode og firmware, der er opdateret.

Personlige computere kan blive inficeret med malware eller ransomware, der kan blokere adgangen til computeren og stjæle følsomme oplysninger. Dette kan også ske via phishing-e-mails eller usikre

downloads. Derfor er det vigtigt at have en stærk antivirussoftware, der kan beskytte mod skadelige angreb.

Smart home-enheder, såsom termostater, dørklokker og overvågningskameraer, er også udsatte for IT-sikkerhedsrisici, da de ofte er forbundet til internettet og kan blive kompromitteret af angribere. Hackere kan bruge disse enheder som en indgangsvej til at få adgang til det brede hjemmenetværk og stjæle følsomme oplysninger eller udføre skadelige handlinger. Derfor er det vigtigt at sikre, at smart home-enheder er beskyttet med stærke adgangskoder og er opdateret med den seneste firmware.

Wi-Fi Access Points (AP) er enheder, der tillader trådløs kommunikation mellem enheder og internettet i et hjemme-netværk. De kan også være en kilde til bekymring, da de kan udgøre en potentiel risiko for IT-sikkerhed i hjemmet.
En af de største sikkerhedsrisici ved wi-fi APer er manglen på stærk kryptering. Hvis wi-fi APet ikke har stærk kryptering, kan det let blive kompromitteret af angribere, der ønsker at få adgang til hjemmenetværket. Dette kan føre til en række alvorlige problemer, som listet tidligere. Derfor er det vigtigt at sikre, at wi-fi APet er beskyttet med en stærk kryptering, såsom WPA2.
En anden sikkerhedsrisiko ved wi-fi APer er, at de kan blive brugt som en indgangsvej for angribere til at få adgang til hjemmenetværket. Angribere kan bruge disse svagheder til at kompromittere wi-fi APet og få adgang til det brede hjemmenetværk. Derfor er det vigtigt at sikre, at wi-fi APet er beskyttet med en stærk adgangskode, og at standardadgangskoden er blevet ændret.
En anden sikkerhedsrisiko ved wi-fi APer er, at de kan være sårbare over for angreb fra en længere afstand. Hackere kan udnytte svagheder i firmwaren eller andre sikkerhedsrelaterede problemer for at få adgang til wi-fi APet og dermed hele hjemmenetværket. Derfor er det også her vigtigt at sikre, at wi-fi APet er opdateret med den seneste firmware, og at eventuelle sårbarheder er blevet rettet.

### 5.2.2 SÅRBAR BRUGERADFÆRD

Udsatte brugeradfærd er en af de største udfordringer i IT-sikkerhed. Det skyldes, at brugerne ofte er det svage led i kæden af sikkerhed i digitale systemer. Brugeradfærd kan være påvirket af mange faktorer, herunder manglende viden om sikkerhed, tidsbegrænsninger og bekvemmelighed. Nogle af de mest almindelige former for sårbar brugeradfærd inkluderer brugen af svage passwords, deling af data, phishing og undladelse af opdatering af software.

Brugere, der bruger svage passwords, kan være et let bytte for hackere, der kan gætte deres passwords eller bryde dem ved hjælp af software. Deling af følsomme data med andre personer kan også føre til, at uautoriserede personer får adgang til disse data og bruger dem til at begå økonomisk svindel eller identitetstyveri. Phishing kan narre brugere til at dele deres følsomme oplysninger med svindlere, der udgiver sig for at være en legitim organisation. Uopdateret software på enheder kan også føre til sikkerhedsproblemer og sårbarheder, der kan udnyttes af hackere.

Udsat brugeradfærd er problematisk, da det kan føre til alvorlige sikkerhedsproblemer i digitale systemer og resultere i økonomiske tab og datatab. Desuden kan det også påvirke tilliden til digitale systemer og organisationer, da brugere kan miste tilliden til organisationer, der ikke tager IT-sikkerhed alvorligt og ikke sikrer, at deres brugere er uddannede i sikkerhedspraksis.

For at minimere risikoen for udsat brugeradfærd i IT-sikkerhed, er det vigtigt at uddanne brugere om relevant sikkerhedspraksis og sørge for, at de har de nødvendige redskaber til at beskytte deres data og enheder. Det inkluderer at vælge stærke passwords, undgå at dele følsomme oplysninger med uautoriserede personer, være opmærksom på phishing og sørge for, at softwaren på ens enheder er opdateret med den seneste version.

## 5.3 NORMALE SIKKERHEDSTILTAG TIL AT FOREBYGGE IT-RELATEREDE TRUSLER

Inden for den hastigt digitaliserede verden er forståelse og integration af robuste sikkerhedspraksisser blevet en essentiel komponent. Fem centrale aspekter af digital sikkerhed er afgørende: opdatering af software og enheder, brugen af stærke passwords og to-faktor-autentifikation, anvendelsen af VPN og kryptering af netværk og data, implementering af firewall og sikkerhedssoftware, samt sikring af e-mail og spamfiltrering. Disse komponenter spiller kritiske roller i beskyttelsen af det digitale fodspor og i opretholdelsen af online sikkerhed. Det er hensigten at formidle disse koncepter på en klar og forståelig måde, og fremhæve deres fundamentale betydning for sikker digital tilstedeværelse.

### 5.3.1 OPDATERING AF SOFTWARE OG ENHEDER

En af de mest fundamentale og effektive strategier til at forebygge it-relaterede trusler er at opdatere software og enheder. Producenter af software og enheder frigiver ofte opdateringer, der indeholder afgørende sikkerhedsrettelser, som kan beskytte mod kendte trusler. Disse opdateringer kan f.eks. lukke sikkerhedshuller eller sårbarheder, som cyberkriminelle kunne udnytte.
Det er af afgørende betydning at sikre, at alle enheder - inklusive computere, telefoner, tablets og andre enheder - har de seneste softwareopdateringer. Det er også vigtigt at aktivere automatiske opdateringer for at modtage opdateringer så snart de bliver tilgængelige.
Det inkluderer også applikationer, såsom PDF-læsere, tekstredigeringsprogrammer og andre potentielle trusselskabere, der kan udnyttes.
Opdateringer kan også indeholde nye funktioner eller forbedringer, der kan hjælpe med at øge produktiviteten eller ydeevnen af enhederne. Ved at holde software og enheder opdateret, forbedres ikke kun sikkerheden, men også brugeroplevelsen og enhedernes ydeevne.

Det er bemærkelsesværdigt, at opdateringer kan afværge trusler, der endnu ikke er opdaget af producenterne eller offentligheden. En ny trussel fremkommer ofte, når cyberkriminelle finder nye metoder til at drage fordel af sårbarheder i software og enheder. Opdateringer, som er udformet til at afværge kendte trusler, kan også omfatte rettelser, der beskytter mod ukendte trusler. Derfor er det essentielt at installere de nyeste opdateringer for at maksimere beskyttelsen mod både kendte og ukendte trusler.
Det er også vigtigt at bemærke, at selvom automatiske opdateringer er praktiske til at sikre, at software og enheder er opdaterede, kan de have uventede problemer. Opdateringer kan for eksempel skabe konflikter med andre programmer eller hardware, hvilket kan resultere i ydeevneproblemer eller systemfejl. Af denne grund er det klogt at tage en sikkerhedskopi af ens data inden der installeres opdateringer og teste opdateringerne på mindre kritiske enheder inden installation på alle enheder.
Sammenfattende kan opdatering af software og enheder betragtes som en af de mest væsentlige sikkerhedsforanstaltninger, som er tilgængelige for at forebygge it-relaterede trusler. Ved regelmæssige og omhyggelige opdateringer kan sårbarheder minimeres og beskyttelse mod kendte og ukendte trusler maksimeres.

### 5.3.2 STÆRKE PASSWORDS OG TO-FAKTOR-AUTENTIFIKATION

Stærke passwords og to-faktor-autentifikation udgør grundlæggende sikkerhedsforanstaltninger, der kan forhindre uautoriseret adgang og misbrug af konti og data. Et stærkt password defineres ved dets unikke karakter og evne til at modstå tilfældige gæt og standardforekomster. Dette betyder, at passwordet ikke bør baseres på almindelige ord, personlige oplysninger eller let tilgængelige informationer. Derudover bør et stærkt password have en tilstrækkelig længde og kompleksitet og bestå af en kombination af bogstaver, tal og specialtegn.
To-faktor-autentifikation er en ekstra sikkerhedsforanstaltning, der kræver brugerens identitet at blive verificeret på to forskellige måder, som ofte involverer en adgangskode samt en kode, der sendes til brugerens telefon eller e-mailadresse. Ved at gennemføre denne proces, forhindres uautoriseret adgang selv i tilfælde af, at en hacker skulle få adgang til ens adgangskode. For at opnå optimal sikkerhed, bør både stærke passwords og to-faktor-autentifikation anvendes på alle konti, særligt de som indeholder følsomme oplysninger såsom bankkonti, IoT-enheder og sociale medier-konti.

Det skal understreges, at mens stærke passwords og to-faktor-autentifikation kan være effektive sikkerhedsforanstaltninger, er de ikke en absolut garanti mod alle it-relaterede trusler. Det er derfor vigtigt, at brugere anvender yderligere sikkerhedsforanstaltninger såsom at undgå at bruge offentlige Wi-Fi-netværk og vedligeholde en opdateret antivirussoftware for at beskytte deres enheder og data mod potentielle trusler.

En udfordring for brugere ved at vælge et godt solidt password er ofte længden. Jo kortere et password er, desto lettere er det at gætte eller bryde det ved hjælp af en software, som er designet til at bryde passwords, eller ved at gætte.
Det anbefales generelt at vælge et password, der er mindst 12 karakterer langt, og som indeholder en kombination af bogstaver, tal og specialtegn. Men mange brugere finder det besværligt at huske et så langt og komplekst password, og de ender ofte med at bruge det samme password til flere konti eller vælge en meget simpel adgangskode, som er nem at huske, men også nem at gætte eller hacke.
For at løse denne udfordring kan brugere bruge en password-manager, der kan generere stærke og unikke passwords til hver konto, og som kan gemme disse sikkert og krypteret. Dette gør det nemt for brugeren at have et forskelligt og sikkert password til hver konto uden at skulle huske dem alle. Det er også vigtigt at huske, at et godt solid password ikke kun beskytter din konto, men også kan beskytte dine personlige oplysninger og forhindre identitetstyveri.

Når det kommer til IoT-enheder, er der specifikke foranstaltninger, der kan træffes for at sikre stærke passwords og to-faktor autentifikation. En af de primære foranstaltninger er at ændre standard-adgangskoden på enhederne, da disse ofte er lette at gætte for hackere. Det anbefales også at anvende et unikt og stærkt password til hver IoT-enhed til at modstå brute-force-angreb.

To-faktor autentifikation kan også anvendes på nogle IoT-enheder, men dette er ikke en standard funktion på alle enheder. Brugere kan undersøge om denne funktion er tilgængelig på deres enheder og aktivere det, hvis det er muligt. Hvis to-faktor autentifikation ikke er en mulighed, kan brugere overveje andre sikkerhedsforanstaltninger såsom netværkssegmentering[7], der begrænser adgangen til IoT-enheder og gør det sværere for hackere at få adgang til andre enheder på netværket.
Det er vigtigt at huske, at IoT-enheder kan udgøre en sårbarhed i et netværk, og derfor er det essentielt at sikre dem på samme niveau som andre enheder, der bruges til at opbevare og behandle følsomme oplysninger. Det anbefales også at holde firmwaren på IoT-enheder opdateret, da nye opdateringer ofte inkluderer sikkerhedsopdateringer og patcher til kendte sårbarheder. Samlet set er det vigtigt at tage de

[7] Netværkssegmentering er en metode til at opdele et netværk i mindre og mere isolerede segmenter for at øge sikkerheden og begrænse muligheden for cyberangreb og spredning af malware.

nødvendige foranstaltninger for at sikre, at IoT-enheder ikke udgør en potentiel trussel mod netværkssikkerheden.

### 5.3.3 VPN OG KRYPTERING AF NETVÆRK OG DATA

Virtual Private Network (VPN)[8] og kryptering af netværk samt data udgør to primære sikkerhedstiltag, som både virksomheder og enkeltpersoner kan implementere for at beskytte sig mod IT-relaterede trusler. Disse teknologier er essentielle for at etablere sikre forbindelser og garantere, at data ikke opsnappes eller ændres under transmission.

VPN fungerer ved at etablere en krypteret forbindelse mellem to enheder over internettet, skabende en sikker tunnel mellem enheden og den tilknyttede VPN-server. Al data sendt og modtaget er krypteret og beskyttet mod uautoriseret adgang, hvilket sikrer, at internettrafik ikke kan overvåges eller stjæles af hackere eller andre tredjeparter. Kryptering af netværk og data indebærer anvendelse af krypteringsalgoritmer for at sikre, at data er ulæselige og uforståelige for uautoriserede personer. Dette inkluderer kryptering af trådløse netværk, e-mail-kommunikation, gemte filer og mapper samt kryptering af hele harddiske.

Valg af passende teknologier og værktøjer er afgørende ved implementering af VPN og kryptering af netværk samt data. Forskellige VPN-tjenester og krypteringsalgoritmer er til rådighed, og det er afgørende at undersøge og vælge de mest sikre og pålidelige løsninger. Generelt er VPN og kryptering af netværk og data afgørende sikkerhedsforanstaltninger, som alle virksomheder og enkeltpersoner bør implementere for at beskytte sig mod IT-relaterede trusler.

Disse teknologier er også relevante for IoT-enheder, som ofte er forbundet til internettet og kan være sårbare over for cybertrusler uden tilstrækkelig beskyttelse. VPN kan skabe en sikker og krypteret forbindelse mellem IoT-enheder og netværket, hvilket muliggør sikker dataoverførsel uden risiko for opsnappet eller ændret data. Kryptering af netværk og data på IoT-enheder kan yderligere beskytte mod hacking, phishing og malware-angreb. Valg af passende VPN- og krypteringsløsninger til IoT-enheder er vigtigt, da begrænsede ressourcer og kapaciteter kan påvirke enhedernes ydeevne og driftssikkerhed. Dog findes der VPN-tjenester og krypteringsalgoritmer designet specifikt til IoT-enheder, som sikrer både pålidelighed og sikkerhed.

### 5.3.4 FIREWALL OG SIKKERHEDSSOFTWARE

I en verden, hvor teknologien er i konstant udvikling, er det vigtigt at være opmærksom på de potentielle trusler, der kan opstå som følge af IT-relaterede angreb. En af de mest grundlæggende og effektive metoder til at sikre dine digitale enheder og netværk er ved at implementere en firewall og sikkerhedssoftware.

En firewall fungerer som et beskyttende skjold mellem dine digitale enheder og det eksterne internet. Den kontrollerer den indgående og udgående trafik, og blokerer uautoriseret adgang, hvilket hjælper med at forhindre uønskede trusler som hackere og malware. Firewalls kan være hardwarebaserede, softwarebaserede eller en kombination af begge. Hardwarebaserede firewalls er fysiske enheder, der er tilsluttet netværket, mens softwarebaserede firewalls er programmer, der kører på dine digitale enheder.

Sikkerhedssoftware er en anden vigtig komponent i beskyttelsen mod IT-relaterede trusler. Disse programmer, såsom antivirus- og antispyware-software, hjælper med at opdage, isolere og fjerne skadelig kode, der kan inficere dine enheder. Mange sikkerhedssoftware-pakker indeholder også

[8] Kryptering af netværk involverer brug af krypteringsalgoritmer til at sikre, at data ikke kan læses eller forstås af uautoriserede personer, når det overføres over netværket f.eks. HTTPS (TLS).

funktioner som spamfiltrering, adgangskontrol og forældrekontrol for at give en endnu mere omfattende beskyttelse.

For at sikre optimal beskyttelse bør følgende praksis overholdes:

- Opdatering: Sørg for, at firewall og sikkerhedssoftware altid er opdateret med de nyeste sikkerhedsopdateringer og -patches. Dette hjælper med at beskytte mod nye og avancerede trusler.
- Konfiguration: Konfigurer dine firewall-indstillinger korrekt for at sikre, at kun autoriseret trafik tillades, og at mistænkelig trafik blokeres effektivt.
- Overvågning: Hold øje med dine digitale enheder og netværk for at opdage eventuelle usædvanlige aktiviteter eller tegn på et angreb. Dette vil give dig mulighed for at reagere hurtigt og begrænse eventuelle skader.
- Uddannelse: Selvuddannelse og undervisning af andre brugere af digitale enheder og netværk om IT-sikkerhed og potentielle trusler er essentielt. Opmærksomhed på disse trusler samt strategier for at undgå dem, udgør et vigtigt skridt i beskyttelsen af data og enheder.

Det er vigtigt at bemærke, at en firewall og sikkerhedssoftware alene ikke er tilstrækkelige til at beskytte mod alle IT-trusler. En omfattende og integreret tilgang til IT-sikkerhed er nødvendig, hvilket inkluderer regelmæssig opdatering af software og styresystemer, stærke adgangskoder, to-faktor-autentificering og regelmæssig backup af vigtige data. Sammenfattende er en firewall og sikkerhedssoftware grundlæggende dele af enhver IT-sikkerhedsstrategi, der kan beskytte mod mange almindelige trusler. Valget af de rigtige værktøjer og korrekt konfiguration af disse er essentielt for at opnå den bedst mulige beskyttelse mod IT-trusler.

### 5.3.5 E-MAIL-SIKKERHED OG SPAMFILTRERING

E-mail-kommunikation udgør en central del af den daglige interaktion til både personlige og professionelle formål. Imidlertid er e-mail også en væsentlig kilde til it-relaterede trusler, herunder phishing-angreb, malware og spam. Det er derfor essentielt at implementere effektive sikkerhedsforanstaltninger og spamfiltreringssystemer for at beskytte individet og dets familiemedlemmer mod potentielle trusler. I det følgende vil der blive præsenteret nogle grundlæggende metoder til at sikre e-mail-kommunikation og reducere risikoen for eksponering for it-trusler.

- Valg af en sikker e-mail-udbyder: Det anbefales at vælge en e-mail-udbyder, som tilbyder et højt sikkerhedsniveau samt beskyttelse mod spam og phishing. Sådanne udbydere benytter avancerede filtreringsteknologier og algoritmer til at identificere og blokere mistænkelige e-mails, inden de når brugerens indbakke.
- Aktivering af to-faktor-autentificering (2FA): To-faktor-autentificering er en supplerende sikkerhedsforanstaltning, der kræver både en adgangskode og en engangskode, der sendes til en sekundær enhed (f.eks. en mobiltelefon), for at opnå adgang til e-mail-kontoen. Implementering af 2FA komplicerer væsentligt muligheden for uautoriseret adgang til kontoen, selv hvis adgangskoden er kompromitteret.
- Identifikation af phishing-e-mails: Phishing-angreb indebærer forsøg på at lokke brugeren til at afsløre personlige oplysninger, såsom adgangskoder og kreditkortoplysninger, ved at give indtryk af, at e-mailen stammer fra en legitim kilde. Det er vigtigt at kunne genkende indikatorer for phishing, såsom grammatikfejl, ukorrekte logoer og mistænkelige e-mailadresser.
- Anvendelse af stærke adgangskoder: Robuste adgangskoder er en afgørende komponent i e-mail-sikkerheden. En stærk adgangskode bør bestå af en kombination af bogstaver, tal og specialtegn, der gør den svær at gætte. Det anbefales at ændre adgangskoder regelmæssigt og undgå at anvende den samme adgangskode på flere konti.

- Opdatering af software: Det er vigtigt at holde computeren, smartphone og e-mail-klient opdateret med de nyeste sikkerhedsrettelser og opdateringer. Flere it-trusler udnytter sårbarheder i forældet software.

For at opsummere er e-mail-sikkerhed og spamfiltrering centrale elementer i beskyttelsen mod it-relaterede trusler for den almindelige bruger i hjemmet. Ved at vælge en sikker e-mail-udbyder, aktivere to-faktor-autentificering, identificere phishing-forsøg, anvende stærke adgangskoder, opdatere software og udvise forsigtighed ved åbning af vedhæftede filer og links, kan brugeren reducere risikoen for eksponering for potentielle trusler. Desuden bør en antivirus- og anti-malware-løsning installeres for at øge beskyttelsen yderligere. Ved at følge disse retningslinjer kan den almindelige bruger sikre en mere sikker og problemfri e-mail-oplevelse og mindske risikoen for kompromittering af personlige oplysninger og data.

## 5.4 IOT-ENHEDER I HJEMMET OG DERES SIKKERHEDSUDFORDRINGER

IoT-enheder refererer til et netværk af forbundne enheder, der kommunikerer og interagerer med hinanden via internettet. Disse enheder spiller en stadig større rolle i moderne hjem, hvor de bidrager til automatisering, energioptimering og forbedret livskvalitet. Imidlertid er der væsentlige udfordringer forbundet med implementeringen af IoT-enheder i hjemmet, navnlig med hensyn til sikkerhed og privatliv.

### 5.4.1 HVAD ER IOT-ENHEDER OG HVORDAN FUNGERER DE I HJEMMET?

IoT-enheder i hjemmet har revolutioneret vores dagligdag på mange måder. De tilbyder en bred vifte af fordele, men det er også vigtigt at være opmærksom på de potentielle ulemper og risici, der følger med deres brug.

#### *5.4.1.1 Bekvemmelighed*

Bekvemmelighed er en afgørende faktor i det daglige liv, og IoT-enheder i hjemmet har betydeligt forstærket denne bekvemmelighed. IoT-enheder har revolutioneret udførelsen af forskellige hjemmeopgaver og interaktion med omgivelserne. I IoT-enhedernes bekvemmelighedsaspekter findes adskillige områder, hvor deres indflydelse kan observeres.
For det første har IoT-enheder muliggjort centralisering af kontrol over forskellige systemer og apparater, hvilket letter justering af indstillinger og aktivering eller deaktivering af funktioner via en enkelt grænseflade, såsom en smartphone-app eller stemmestyret assistent. F.eks. kan belysning, termostater, gardiner og dørlåse styres ved hjælp af en smartphone eller stemmekommando [20]. Derudover tillader IoT-enheder en højere grad af personalisering af boligindstillinger. Ved at lære af præferencer og rutiner kan disse enheder automatisk justere indstillinger og funktioner for at skabe en behagelig og bekvem atmosfære. IoT-enheder letter også styring og vedligeholdelse af hjemmet, f.eks. ved at sende notifikationer fra intelligente vaskemaskiner og tørretumblere eller ved at lade robotstøvsugere rengøre gulve, mens beboerne er på arbejde, frigørende tid og energi til andre aktiviteter [21].

IoT-enheder kan forbedre arbejdsliv og fritid ved at skabe det ideelle fysiske miljø for arbejde, hvilket kan øge produktivitet og trivsel. Disse enheder kan også forbedre fritidsoplevelsen ved nemt at styre underholdningssystemer, som fjernsyn, lydsystemer og spillekonsoller.
Sammenfattende har IoT-enheder i hjemmet medført hidtil uset bekvemmelighed og kontrol over boligindstillinger, hvilket gør det nemmere at tilpasse hjemmet til individuelle præferencer og behov. Dette har resulteret i en mere behagelig, effektiv og tilpasset hverdag for mange mennesker. IoT-enheder i hjemmet bidrager også til mere intelligente og bæredygtige hjem ved at optimere energiforbrug og ressourcestyring, hvilket ikke kun øger bekvemmeligheden, men også fremmer en miljøvenlig livsstil. Endelig er bekvemmeligheden ved IoT-enheder særligt gavnlig for personer med begrænset mobilitet eller særlige behov, som kan drage fordel af den øgede kontrol og tilpasningsevne,

som disse enheder tilbyder, potentielt forbedrende livskvalitet og uafhængighed for disse individer og deres familier betydeligt [22].

På trods af bekvemmeligheden ved IoT-enheder i hjemmet og de mange fordele, de tilbyder, er det vigtigt at være opmærksom på de potentielle risici og ulemper, der kan opstå, herunder sikkerheds- og privatlivsbekymringer. Ved at træffe de nødvendige forholdsregler og omhyggeligt vælge IoT-enheder, er det muligt at nyde den øgede bekvemmelighed og kontrol, som disse enheder giver, samtidig med at privatliv og sikkerhed bevares.

#### *5.4.1.2 Tilgængelighed og komfort i hjemmet for personer med særlige behov*

Integrationen af IoT-enheder i hjemmet har potentielt betydelige fordele for ældre og handicappede personer, der søger at opretholde deres uafhængighed og livskvalitet. Disse teknologier kan lette daglige opgaver og give et højere niveau af komfort og sikkerhed for personer med begrænset mobilitet eller særlige behov.

#### *5.4.1.3 Forbedret sikkerhed*

IoT-enheder kan spille en afgørende rolle i forbedringen af hjemmets sikkerhed. Integrationen af teknologier som sikkerhedskameraer, bevægelsessensorer og smarte låse i hjemmets økosystem kan skabe et mere robust og proaktivt forsvar mod uvedkommende og potentielle trusler. Disse avancerede teknologier kan overvåge hjemmet i realtid og give nøjagtige og rettidige advarsler om mistænkelige aktiviteter, hvilket bidrager til at opretholde et sikkert og trygt miljø.
Sikkerhedskameraer, for eksempel, kan overvåge og optage aktiviteter i og omkring hjemmet kontinuerligt, hvilket gør det muligt at identificere mistænkelige personer og handlinger. Bevægelsessensorer kan registrere bevægelse i specifikke områder og aktivere alarmer eller notifikationer, når uautoriseret adgang forsøges. Smarte låse, der kan styres fra smartphones, giver beboerne mulighed for at låse og låse op for døre, selv når de ikke er hjemme, og kan give midlertidig adgang til gæster eller servicemedarbejdere.
Selvom IoT-enheder kan bidrage til at øge sikkerheden i hjemmet, er det vigtigt at tage højde for de potentielle it-sikkerhedsudfordringer, der kan opstå som følge af deres anvendelse. IoT-enheder er ofte forbundet til internettet og kan derfor være sårbare over for cyberangreb og hacking. Dette kan føre til kompromittering af personlige oplysninger og kontrol over hjemmets sikkerhedssystemer.
For at afbøde disse risici er det vigtigt at sikre, at de valgte IoT-enheder følger strenge sikkerhedsstandarder og har opdaterede sikkerhedsprotokoller. Det kan også være nyttigt at have et lag af beskyttelse, såsom en firewall eller et virtuelt privat netværk (VPN), for at forhindre uautoriseret adgang til hjemmets netværk. Desuden er det vigtigt at opretholde god praksis for adgangskodeadministration og regelmæssigt opdatere enhedernes firmware for at beskytte mod kendte sårbarheder.
I sidste ende kan IoT-enheder bidrage til en forbedret sikkerhed i hjemmet, men det er vigtigt at være opmærksom på de potentielle it-sikkerhedsudfordringer og træffe passende foranstaltninger for at sikre, at hjemmet forbliver beskyttet. Ved at finde en balance mellem de fordele, som IoT-enheder kan tilbyde, og de risici, de kan medføre, er det og de risici, de kan medføre, er det muligt at skabe et sikkert og beskyttet hjemmemiljø på et oplyst grundlag udfra de nyeste teknologiske fremskridt inden for sikkerhedsforanstaltninger.

For at opsummere er der mange fordele ved at integrere IoT-enheder i hjemmets sikkerhedssystemer. Når de implementeres korrekt, kan disse enheder øge beskyttelsen af boligen og dens beboere ved at tilbyde proaktiv overvågning, realtidsalarmer og fleksibel adgangskontrol. Samtidig er det vigtigt at være opmærksom på de potentielle it-sikkerhedsudfordringer og tage passende skridt for at sikre, at disse enheder forbliver sikre og pålidelige. Ved at kombinere de nyeste IoT-teknologier med omhyggelig planlægning og opmærksomhed på sikkerhed kan et hjem blive et mere sikkert og trygt sted for beboerne.

### 5.4.2 TRUSLER MOD IOT-SIKKERHED

På trods af de mange fordele, IoT-teknologi bringer med sig, er der også en række sikkerhedstrusler og udfordringer, som skal tages i betragtning. Disse trusler inkluderer hacking, datamisbrug og sikkerhedsbrister i enheder.

Hacking er en af de mest prominente trusler mod IoT-sikkerhed. Uautoriserede aktører kan forsøge at få adgang til IoT-enheders data, enten for at afbryde deres funktion, stjæle information eller udføre ondsindede handlinger. På grund af mangfoldigheden af IoT-enheder og deres udbredte anvendelse, er angrebsoverfladen for hackere betydeligt forøget. Dette skaber en kompleks udfordring for at beskytte IoT-enheder mod cyberangreb og kræver konstant opdatering af sikkerhedsprotokoller og -foranstaltninger.

IoT-enheder indsamler og genererer store mængder data, som kan være meget værdifulde for både legitime og illegitime aktører. Uautoriseret adgang til disse data kan føre til misbrug, såsom at spore folks bevægelser og adfærd, stjæle personlige oplysninger, eller udnytte data til kommercielle eller politiske formål. Dette rejser spørgsmål om beskyttelse af personlige oplysninger og datasikkerhed, der kræver omfattende juridiske og tekniske løsninger.

Mange IoT-enheder har sikkerhedsbrister på grund af utilstrækkelige eller forældede sikkerhedsprotokoller og -foranstaltninger. Årsagerne til disse brister kan omfatte manglende opdateringer, svage adgangskoder, manglende kryptering og utilstrækkelig segmentering af netværket. Disse sikkerhedsbrister gør det muligt for uautoriserede aktører at udnytte sårbarheder og kompromittere IoT-enheder og de systemer, de er en del af.

### 5.4.3 SIKKERHEDSTILTAG TIL AT BESKYTTE IOT-ENHEDER

Sikkerhedstiltag, der kan implementeres for at beskytte IoT-enheder, omfatter flere strategier og praksisser. Adgangskontrol er afgørende for at sikre, at kun autoriserede brugere får adgang til enheder og de data, de genererer. Dette kan opnås ved at implementere robuste adgangskoder, to-faktor-autentificering og biometrisk identifikation.
Softwareopdateringer er også et vigtigt sikkerhedstiltag, da de hjælper med at holde enhedernes systemer opdaterede og beskyttede mod kendte sårbarheder. Ved regelmæssigt at installere opdateringer fra producenterne kan brugere forhindre udnyttelse af svagheder i deres IoT-enheder. Det anbefales at aktivere automatiske opdateringer, når det er muligt, for at minimere risikoen for forældet software.

Netværkssikkerhed er en yderligere metode til at beskytte IoT-enheder, da det forhindrer uautoriseret adgang og kontrol over enhederne via netværket. En grundlæggende foranstaltning er at sikre, at hjemmenetværket er beskyttet med en stærk adgangskode og kryptering, såsom WPA2 eller WPA3. Desuden kan segmentering af netværket, hvor IoT-enheder isoleres fra andre dele af netværket, reducere risikoen for, at en kompromitteret enhed kan påvirke andre enheder eller systemer. Yderligere sikkerhedspraksis inkluderer regelmæssig overvågning af IoT-enheder for mistænkelig aktivitet, begrænsning af dataindsamling til det strengt nødvendige og brug af sikkerhedssoftware, såsom firewalls og antivirusprogrammer. Ved at tage disse forholdsregler kan brugere minimere risikoen for sikkerhedsbrud og beskytte deres IoT-enheder mod potentielle trusler [23].

#### *5.4.3.1 Det er udfordrende for brugere til at implementere sikkerhed*

Sikkerhedsudfordringer for den almene person i forbindelse med IoT-enheder kan tilskrives flere faktorer, som gør det vanskeligt for dem at navigere i kompleksiteten af digital sikkerhed. Disse faktorer inkluderer teknisk viden, tidsforbrug og manglende bevidsthed om trusler og konsekvenser.
For det første kan begrænset teknisk viden hos almindelige brugere gøre det vanskeligt at implementere de nødvendige sikkerhedsforanstaltninger. IoT-enheder kan variere betydeligt i deres funktionalitet og

sikkerhedskrav, hvilket kan skabe forvirring for brugere, der ikke har en baggrund inden for informationsteknologi eller cybersikkerhed.
For det andet kan tidsforbruget i forbindelse med at vedligeholde og opdatere IoT-enheder og deres sikkerhed være en udfordring for den almene person. Det kræver en løbende indsats at holde sig ajour med softwareopdateringer, oprette lange adgangskoder regelmæssigt og overvåge enheder for mistænkelig aktivitet, hvilket kan blive en byrde for brugere med begrænset tid og ressourcer.
For det tredje er der ofte en mangel på bevidsthed om de potentielle trusler og konsekvenser af utilstrækkelig IoT-sikkerhed. Uden en klar forståelse af risiciene kan den almene person undervurdere betydningen af at beskytte deres enheder og data. Dette kan føre til manglende motivation for at implementere passende sikkerhedsforanstaltninger.

Disse faktorer i kombination bidrager til udfordringen for almindelige brugere i effektivt at sikre deres IoT-enheder. Dette understreger betydningen af at forhøje bevidstheden om sikkerhedsrisici og uddanne brugere om de mest effektive metoder til at beskytte deres IoT-enheder og hjemmenetværk mod potentielle trusler.

## 5.5 ISO 27001 OG SIKKERHEDSLEDELSE I HJEMMET

ISO 27001 [17] og sikkerhedsledelse i hjemmet er et relevant emne, der fokuserer på, hvordan principperne fra den internationale standard for informationssikkerhed kan tilpasses og anvendes i en hjemmeindstilling. Selvom ISO 27001 primært er designet til organisationer og virksomheder, kan dets retningslinjer og praksis have en positiv indvirkning på IT-sikkerheden i hjemmet, når de tilpasses korrekt. Ved at implementere en systematisk tilgang til sikkerhedsledelse og tage højde for risikovurdering, adgangskontrol, sikkerhedsopdateringer og bevidstgørelse kan husejere skabe et mere sikkert og beskyttet hjemmemiljø for deres IT-systemer og -enheder.

### 5.5.1 ISO 27001: ANVENDELSE I HJEMME-IT SIKKERHED

ISO 27001 er en international standard for informationssikkerhed, der er udviklet og vedligeholdt af den Internationale Organisation for Standardisering (ISO). Standarden specificerer kravene til et Informationssikkerhedsledelsessystem (ISMS), som er en systematisk tilgang til at styre og beskytte fortrolige data og minimere risikoen for sikkerhedsbrud og datatab. ISO 27001 fokuserer på at identificere, vurdere og behandle sikkerhedsrisici i en organisation og hjælper virksomheder med at opbygge en stærk informationsbeskyttelseskultur.
Når det kommer til IT-sikkerhed i hjemmet, er ISO 27001 primært rettet mod virksomheder og organisationer og ikke direkte anvendelig på husstande. Dog kan nogle af principperne og fremgangsmåderne fra ISO 27001 være nyttige for at styrke IT-sikkerheden i hjemmet, selvom det ikke er en perfekt pasform. Her er nogle måder, hvorpå ISO 27001 principper kan anvendes i hjemmet:

- **Risikovurdering**: Ligesom virksomheder skal vurdere deres risici i forbindelse med informationssikkerhed, kan husstande også gennemføre en grundlæggende risikovurdering for at identificere potentielle trusler mod deres IT-systemer og -enheder.
- **Adgangskontrol**: ISO 27001 indeholder retningslinjer for styring af adgang til informationssystemer. Husejere kan anvende disse principper ved at sikre, at adgang til computere og netværk er begrænset til autoriserede brugere, og at stærke adgangskoder og to-faktor-autentifikation anvendes, hvor det er muligt.
- **Sikkerhedsopdateringer og patch management**: At holde software og firmware opdateret er afgørende for at beskytte mod kendte sårbarheder. Husejere kan sikre, at deres IT-systemer og -enheder modtager regelmæssige opdateringer og patches for at minimere risikoen for sikkerhedsbrud.
- **Sikkerhedspolitikker**: Selvom hjemmebrugere ikke nødvendigvis behøver at have en formel sikkerhedspolitik, kan det være nyttigt at have grundlæggende retningslinjer for, hvordan IT-systemer og -enheder skal bruges og beskyttes. Dette kan omfatte at undgå at klikke på

mistænkelige links, downloade software fra upålidelige kilder og dele personlige oplysninger med ukendte parter.

Selvom ISO 27001 primært er designet til virksomheder og organisationer, kan nogle af dets principper og praksis anvendes i mindre skala for at forbedre IT-sikkerheden i hjemmet. Det er dog vigtigt at tage højde for, at hjemmebrugere kan have forskellige behov og begrænsninger, og at nogle af ISO 27001's aspekter måske ikke er direkte anvendelige eller nødvendige i en hjemmeindstilling. Det er derfor vigtigt at tilpasse disse principper og praksis til de specifikke krav og udfordringer i forbindelse med IT-sikkerhed i hjemmet.

- **Fysisk sikkerhed**: ISO 27001 indeholder også retningslinjer for at beskytte IT-udstyr og infrastruktur mod fysisk skade og uautoriseret adgang. Husejere kan tage højde for dette ved at opbevare udstyr som computere, routere og eksterne lagringsenheder på sikre steder, beskytte mod overspænding og installere sikkerhedslåse på døre og vinduer, hvor det er relevant.
- **Sikker opbevaring og destruktion af data**: Det er vigtigt at opbevare data sikkert og at slette dem forsvarligt, når de ikke længere er nødvendige. Husejere kan anvende kryptering og sikkerhedskopiering af data samt anvende sikker sletning af data på elektroniske medier, når de skal bortskaffes.
- **Bevidstgørelse og uddannelse**: En vigtig del af ISO 27001 er at øge bevidstheden om informationssikkerhed og uddanne medarbejdere om sikkerhedspraksis. Husejere og familiemedlemmer kan drage fordel af denne tilgang ved at holde sig informeret om aktuelle trusler og bedste praksis for IT-sikkerhed samt dele denne viden med andre familiemedlemmer.
- **Incident management**: At have en plan for håndtering af sikkerhedsbrud og datatab er en vital del af ISO 27001. Husejere kan udforme en enkel plan for respons på potentielle sikkerhedshændelser, der inkluderer kontaktinformationer, skridt til at begrænse skaden, samt procedurer for genopretning af systemer og data.

Selvom ISO 27001 er designet til organisationer og virksomheder, kan dets principper og praksis, når de tilpasses og anvendes i mindre skala, bidrage til at forbedre IT-sikkerheden i hjemmet. Ved at tage højde for disse aspekter og tilpasse dem til hjemmebrugernes specifikke behov kan husejere opnå en mere sikker og robust IT-infrastruktur og beskytte deres data mod uautoriseret adgang og misbrug.

### 5.5.2 IMPLEMENTERING AF ISO 27001 I HJEMMET OG DENS FORDELE SAMT ULEMPER

Implementering af ISO 27001 i hjemmet indebærer at tilpasse principperne og praksis fra denne internationale standard for informationssikkerhed til de specifikke behov og udfordringer, som hjemmebrugere står over for. Selvom ISO 27001 primært er rettet mod virksomheder og organisationer, kan dets koncepter have en positiv indvirkning på IT-sikkerheden i hjemmet, når de tilpasses korrekt. Nedenfor er nogle fordele og ulemper ved at implementere ISO 27001 i hjemmet.

Fordele:

- **Forbedret IT-sikkerhed**: Ved at følge ISO 27001-principperne kan husejere opnå en højere grad af sikkerhed for deres IT-systemer og -enheder, hvilket reducerer risikoen for cyberangreb og datatab.
- **Systematisk tilgang**: ISO 27001 fremmer en systematisk tilgang til håndtering af informationssikkerhed, hvilket kan hjælpe husejere med at identificere og prioritere potentielle trusler og implementere passende sikkerhedsforanstaltninger.
- **Bevidstgørelse og uddannelse**: Implementering af ISO 27001 i hjemmet kan øge bevidstheden om IT-sikkerhed og fremme bedre praksis blandt familiemedlemmer, hvilket styrker det samlede sikkerhedsniveau.
- **Kontinuerlig forbedring**: ISO 27001 opfordrer til kontinuerlig forbedring af informationssikkerhedsledelsessystemet, hvilket kan hjælpe husejere med at holde trit med ændringer i trusselsbilledet og teknologiske fremskridt.

Ulemper:

- **Ressourcekrævende**: Implementering af ISO 27001 i hjemmet kan kræve en betydelig investering af tid og andre ressourcer, hvilket kan være en udfordring for husejere med begrænsede ressourcer eller teknisk ekspertise.
- **Kompleksitet**: ISO 27001 er en omfattende standard, der indeholder mange krav og kontrolforanstaltninger. Dens kompleksitet kan gøre det vanskeligt for husejere at forstå og implementere alle aspekter af standarden fuldt ud.
- **Manglende relevans**: Nogle dele af ISO 27001 er måske ikke direkte relevante eller nødvendige for hjemmebrugere, hvilket kan føre til unødvendig kompleksitet og indsats.
- **Ingen officiel certificering**: Implementering af ISO 27001 i hjemmet vil ikke føre til en officiel certificering, som det ville for en organisation eller virksomhed. Dette betyder, at de opnåede fordele ved implementeringen primært, vil være interne og ikke anerkendt af eksterne parter.

Sammenfattende kan implementering af ISO 27001 i hjemmet medføre fordele såsom forbedret IT-sikkerhed og en systematisk tilgang til håndtering af informationssikkerhedsrisici. Dog kan det også indebære ulemper som ressourcekrav, kompleksitet og manglende relevans for nogle aspekter af standarden. For at opnå den optimale balance mellem fordele og ulemper kan husejere overveje at tilpasse ISO 27001-principperne og praksis til deres specifikke behov og kapaciteter, frem for at forsøge at følge standarden fuldt ud. Dette vil gøre det muligt at fokusere på de mest relevante og effektive sikkerhedsforanstaltninger og skabe et mere sikkert og beskyttet hjemmemiljø for IT-systemer og -enheder.

### 5.5.3 UDFORDRINGER VED AT IMPLEMENTERE ISO 27001 I HJEMMET

Implementering af ISO 27001 i hjemmet kan præsentere diverse udfordringer, idet standarden primært er designet for organisationer og virksomheder. Her følger nogle af de mest gængse udfordringer sammen med forslag til deres håndtering:

- **Ressourcekrav**: Implementering af ISO 27001 i hjemmet kan kræve betydelige ressourcer, både i form af tid og omkostninger. For at håndtere dette kan husejere fokusere på de mest relevante og effektive sikkerhedsforanstaltninger, der er tilpasset deres specifikke behov, og prioritere disse tiltag.
- **Teknisk ekspertise**: ISO 27001 kan kræve en vis grad af teknisk viden for at implementere og vedligeholde korrekt. Husejere kan søge hjælp fra IT-sikkerhedseksperter eller læse op på online ressourcer og vejledninger for at øge deres forståelse og kompetencer.
- **Manglende relevans**: Nogle dele af ISO 27001 er muligvis ikke direkte relevante eller nødvendige for hjemmebrugere. For at håndtere dette kan husejere tilpasse standardens principper og praksis til deres specifikke situation og fokusere på de aspekter, der er mest relevante og gavnlige for dem.
- **Kontinuerlig forbedring**: Opdatering og vedligeholdelse af informationssikkerhedsledelsessystemet kan være tidskrævende og krævende. For at imødekomme dette kan husejere planlægge regelmæssige gennemgange og opdateringer af deres IT-sikkerhedstiltag og holde sig informeret om nye trusler og teknologier.
- **Motivation og engagement**: Det kan være udfordrende at engagere alle familiemedlemmer i IT-sikkerhedsprocessen og opretholde en høj grad af bevidsthed om informationssikkerhed. For at overvinde dette kan husejere fremme en sikkerhedskultur gennem uddannelse, kommunikation og opmuntring af ansvarlighed.
- **Praktisk implementering**: At omsætte ISO 27001-principperne til konkrete handlinger i hjemmet kan være en udfordring. For at løse dette kan husejere udarbejde en detaljeret handlingsplan, der indeholder specifikke trin og mål for at forbedre deres IT-sikkerhed.

Ved at håndtere disse udfordringer på en proaktiv og pragmatisk måde kan husejere implementere ISO 27001-principperne og praksis i hjemmet på en måde, der er tilpasset deres specifikke behov og kapaciteter. Dette vil gøre det muligt at opnå en højere grad af IT-sikkerhed og beskyttelse mod potentielle trusler, samtidig med at ressourcekrav og kompleksitet holdes på et minimum.

## 5.6 IMPLEMENTERING AF ISO 27001 I HJEMMET

Implementering af ISO 27001, den internationale standard for informationssikkerhed, i et hjemmemiljø præsenterer en række udfordringer. Emnet for diskussion er de nødvendige krav for en sådan implementering og realismen af dette foretagende. At forstå de konkrete betingelser og potentielle hindringer forbundet med introduktionen af en så kompleks og omfattende standard i en privat bolig er afgørende. Dette kan medvirke til at gøre beslutningen om, hvorvidt ISO 27001 er egnet og hensigtsmæssig til implementering i hjemmet, mere informeret.

### 5.6.1 KRAVENE FOR AT IMPLEMENTERE ISO 27001 I HJEMMET

Implementering af ISO 27001 i hjemmet er en proces, der indebærer en række krav og anbefalinger for at opnå et højt niveau af informationssikkerhed og privatlivets fred. ISO 27001 er en international standard for styring af informationssikkerhed, der beskriver bedste praksis for etablering, implementering, vedligeholdelse og forbedring af et Informationssikkerhedsledelsessystem (ISMS). Selvom ISO 27001 primært er rettet mod virksomheder og organisationer, kan principperne og kravene i standarden også tilpasses til hjemmemiljøet for at beskytte personlige data og netværk.
For at implementere ISO 27001 i hjemmet, er det først nødvendigt at forstå de grundlæggende principper og krav i standarden. ISO 27001 er baseret på en risikobaseret tilgang, der fokuserer på at identificere og vurdere de potentielle trusler og sårbarheder, der kan påvirke informationssikkerheden. Dette indebærer at foretage en risikovurdering, der tager hensyn til alle relevante aspekter af hjemmet, såsom fysiske adgangskontroller, netværkssikkerhed, enhedsstyring og brug af cloud-tjenester.

Efter at have identificeret og vurderet risiciene, er det nødvendigt at udvikle en risikohåndteringsplan, der beskriver de nødvendige kontrolforanstaltninger for at reducere eller eliminere risiciene. Kontrolforanstaltningerne kan variere afhængigt af hjemmets specifikke behov og ressourcer, men nogle grundlæggende foranstaltninger kan omfatte stærkere adgangskontrol (f.eks. komplekse adgangskoder og to-faktor-autentificering), kryptering af data, sikkerhedskopiering af vigtige filer og regelmæssige opdateringer af software og firmware.

I overensstemmelse med ISO 27001's krav om løbende forbedring er det vigtigt at overvåge og evaluere effektiviteten af de implementerede kontrolforanstaltninger. Dette kan indebære regelmæssige sikkerhedsrevisioner, overvågning af netværksaktivitet og gennemgang af hændelseslogfiler for at identificere og reagere på eventuelle sikkerhedshændelser. Det er også afgørende at holde sig opdateret om nye trusler og sårbarheder og justere kontrolforanstaltningerne efter behov.
En vigtig del af implementeringen af ISO 27001 i hjemmet er at skabe en kultur af sikkerhed og bevidsthed blandt husstandens medlemmer. Dette kan opnås gennem uddannelse og træning i sikkerhedsprincipper, såsom sikker brug af internettet, beskyttelse af personlige oplysninger og rapportering af mistænkelig aktivitet. Det er også vigtigt at etablere og over holde klare politikker og procedurer for informationssikkerhed, der er tilpasset hjemmets specifikke behov og situation. Disse politikker og procedurer skal gennemgås og opdateres regelmæssigt for at sikre, at de forbliver relevante og effektive.

For at sikre overholdelse af lovgivningen og beskytte privatlivets fred for husstandens medlemmer er det vigtigt at overveje eventuelle juridiske og etiske aspekter ved implementeringen af ISO 27001 i hjemmet. Dette kan omfatte at sikre, at personlige data indsamles, opbevares og behandles i overensstemmelse med gældende lovgivning, såsom databeskyttelsesregler og privatlivets fred. Det er også vigtigt at

respektere de individuelle rettigheder og præferencer for husstandens medlemmer, når det kommer til deres personlige oplysninger og brugen af teknologi.
Implementeringen af ISO 27001 i hjemmet kan kræve betydelige investeringer i tid, ressourcer og teknologi. Det er derfor vigtigt at overveje de potentielle omkostninger og fordele ved at gennemføre et ISMS og at træffe informerede beslutninger om, hvilke kontrolforanstaltninger der er mest hensigtsmæssige og omkostningseffektive for det specifikke hjem. Det er også vigtigt at være realistisk omkring, hvad der kan opnås gennem implementeringen af ISO 27001, da det er usandsynligt, at det vil være muligt at opnå fuldstændig sikkerhed eller at eliminere alle risici.
Sammenfattende indebærer implementeringen af ISO 27001 i hjemmet en række krav og anbefalinger, der skal tilpasses og anvendes i overensstemmelse med de specifikke behov og ressourcer i det pågældende hjem. Dette omfatter identifikation og vurdering af risici, udvikling og implementering af en risikohåndteringsplan, overvågning og evaluering af kontrolforanstaltninger, uddannelse og bevidstgørelse af husstandens medlemmer, overholdelse af lovgivningen og beskyttelse af privatlivets fred samt overvejelse af omkostninger og fordele ved implementeringen. Ved at følge disse retningslinjer og principper kan ISO 27001 hjælpe med at forbedre informationssikkerheden og privatlivets fred i hjemmet og bidrage til at skabe et sikkert og trygt miljø for alle husstandens medlemmer.

Implementering af en simplificeret version af ISO 27001 i hjemmet kan bidrage til at beskytte personlige data og netværk mod potentielle sikkerhedstrusler. Ved at tilpasse grundlæggende principper fra standarden til hjemmets specifikke behov kan husstandens medlemmer opnå et højere niveau af informationssikkerhed. Dette kan inkludere risikovurdering, passende kontrolforanstaltninger og bevidstgørelse om sikkerhedspraksis, hvilket resulterer i et mere sikkert og privat miljø for alle i hjemmet.

### 5.6.2 ER DET REALISTISK AT IMPLEMENTERE ISO 27001 I HJEMMET

Implementering af ISO 27001 i hjemmet i sin fulde form er måske ikke realistisk for de fleste husstande, da standarden primært er designet til virksomheder og organisationer. Implementeringen af ISO 27001 kan kræve betydelige ressourcer, tid og ekspertise, som mange husstande muligvis ikke har til rådighed eller er realistisk.
Dog kan det være realistisk og gavnligt at implementere en forenklet og tilpasset version af ISO 27001 i hjemmet. Ved at tage udgangspunkt i grundlæggende principper og krav fra standarden, såsom risikovurdering, kontrolforanstaltninger og bevidstgørelse om sikkerhedspraksis, kan husstandens medlemmer arbejde på at forbedre informationssikkerheden og privatlivets fred i hjemmet.
I sidste ende afhænger realiseringen af at implementere ISO 27001 i hjemmet af den enkelte husstands ressourcer, tid og engagement samt deres forståelse af og evne til at tilpasse standardens principper til deres specifikke situation.

## 5.7 BEVIDSTHED OG UDDANNELSE OM ISO 27001 I HJEMMET

At uddanne og oplyse familien om ISO 27001 og IT-sikkerhed er afgørende for at beskytte hjemmets digitale miljø og personlige oplysninger. Dette involverer at skabe en kultur af bevidsthed og ansvarlighed gennem forskellige metoder, såsom familiediskussioner, online ressourcer, praktiske øvelser og løbende opdateringer om nye trusler og sikkerhedsanbefalinger. Ved at engagere hele familien i IT-sikkerhedsprocessen bliver det muligt at opbygge et sikkert og trygt digitalt miljø for alle medlemmer af husstanden.

- **Familiediskussioner**: Arranger regelmæssige samtaler med familien om IT-sikkerhed og vigtigheden af at beskytte personlige oplysninger. Introducer ISO 27001-principperne og forklar, hvordan de er relevante for hjemmets sikkerhed.
- **Online ressourcer**: Det anbefales at benytte online ressourcer, såsom vejledninger, videoer og artikler om ISO 27001 og IT-sikkerhed, og dele dem med familiemedlemmer. Det er vigtigt at vælge ressourcer, der er letforståelige og relevante for hjemmemiljøet.

- **Ekspertvejledning**: Det kan være en god idé at konsultere en IT-sikkerhedsekspert eller en ISO 27001-konsulent for vejledning og uddannelse om effektiv implementering af sikkerhedsprincipper i hjemmet.
- **Kursus eller workshop**: Tilmeld familien til et kursus eller en workshop om IT-sikkerhed og ISO 27001, hvor de kan lære om og diskutere sikkerhedsprincipper og bedste praksis.
- **Praktiske øvelser**: Planlæg praktiske øvelser og aktiviteter, der involverer hele familien, såsom at gennemgå hjemmets netværksindstillinger, opdatere adgangskoder og gennemføre sikkerhedskontroller.
- **Sikkerhedspolitikker og procedurer**: Udarbejd og del skriftlige politikker og procedurer for informationssikkerhed i hjemmet, der er baseret på ISO 27001-principperne. Gør dem tilgængelige for hele familien og opfordr dem til at følge retningslinjerne.
- **Løbende opdatering**: Hold familien opdateret om nye trusler, sårbarheder og sikkerhedsanbefalinger ved at dele nyheder, artikler og oplysninger fra pålidelige kilder. Sørg for at opdatere og justere hjemmets sikkerhedsforanstaltninger efter behov.

Ved at anvende disse metoder til at uddanne og oplyse familiemedlemmer om ISO 27001 og IT-sikkerhed, kan der skabes en kultur af bevidsthed og ansvarlighed, som bidrager til at beskytte det digitale miljø i hjemmet og personlige oplysninger.

## 5.8 FREMTIDSPERSPEKTIVER FOR IT-SIKKERHED OG ISO 27001 I HJEMMET

I takt med den stigende digitalisering og afhængighed af teknologi i vores hverdag er IT-sikkerhed og ISO 27001 i hjemmet blevet mere relevante end nogensinde før. I dette afsnit kigges på , hvordan IT-sikkerhed og ISO 27001 i hjemmet kan udvikle sig i fremtiden, samt diskutere de løbende ændringer i risikobilledet og de nye trusler, der kan opstå på daglig basis.

### 5.8.1 HVORDAN KAN ISO 27001 OG IT-SIKKERHED I HJEMMET UDVIKLE SIG I FREMTIDEN?

Fremtidsperspektiver for IT-sikkerhed og ISO 27001 i hjemmet omfatter en række vigtige tendenser og teknologier, som forventes at påvirke både privatpersoner og virksomheder. Med stigende digitalisering og konstante trusler i det digitale landskab er det afgørende at være opmærksom på udviklingen inden for IT-sikkerhed og holde sig ajour med internationale standarder såsom ISO 27001.
Et centralt aspekt i fremtidens IT-sikkerhed og ISO 27001 er den løbende ændring af risikobilledet. Nye trusler opstår dagligt, og både privatpersoner og organisationer skal være proaktive og fleksible i deres tilgang til at beskytte deres digitale aktiver. Nogle af de mest fremtrædende trusler i dag inkluderer ransomware, phishing-angreb og identitetstyveri, men fremtidige trusler kan være mere avancerede og sofistikerede, hvilket nødvendiggør kontinuerlig opdatering af IT-sikkerhedsforanstaltninger og strategier.

I takt med at IoT-enheder bliver mere udbredte i hjemmet, øges kompleksiteten og risikoen for potentielle angreb. Dette skaber et presserende behov for at integrere ISO 27001 og IT-sikkerhed mere omfattende i hjemmet. Forbrugere skal være mere bevidste om de risici, der er forbundet med at have et stort antal forbundne enheder og tage skridt til at beskytte deres personlige oplysninger og netværk.
Kunstig intelligens (AI) og maskinlæring forventes at spille en stor rolle i udviklingen af IT-sikkerhed og ISO 27001 i fremtiden. AI kan hjælpe med at identificere nye trusler og angrebsmetoder hurtigere og mere præcist end menneskelige eksperter. Dette vil give mulighed for en mere proaktiv tilgang til IT-sikkerhed og løbende opdatering af beskyttelsesforanstaltninger.
For at imødekomme de konstante trusselsændringer er det også nødvendigt at styrke samarbejdet mellem offentlige og private organisationer samt mellem lande. Deling af efterretninger om nye trusler og angrebsmetoder kan hjælpe med at skabe en mere robust og samlet front mod cyberkriminalitet.
I forhold til ISO 27001 vil der være et stigende behov for at holde standarden opdateret og relevant i forhold til de skiftende teknologiske og sikkerhedsmæssige udfordringer. Dette kan indebære periodiske

revisioner og opdateringer for at sikre, at standarden fortsat er effektiv og tilpasset det aktuelle risikobillede.

For at imødekomme fremtidens IT-sikkerhed og ISO 27001 i hjemmet er det vigtigt, at både enkeltpersoner og organisationer forstår betydningen af at investere i sikkerhed og tage de nødvendige skridt for at beskytte deres digitale aktiver og privatliv. Dette kan omfatte løbende uddannelse og træning i IT-sikkerhed, opdatering af software og hardware, samt implementering af stærke adgangskodepolitikker og sikkerhedsprotokoller.
Ud over at følge ISO 27001-standarder og investere i de nyeste sikkerhedsteknologier, bør enkeltpersoner og organisationer også fokusere på at skabe en sikkerhedskultur, hvor alle forstår vigtigheden af IT-sikkerhed og deres rolle i at beskytte organisationens eller hjemmets digitale aktiver. Dette indebærer at skabe bevidsthed om potentielle trusler og uddanne medarbejdere og familiemedlemmer i bedste praksis for at minimere risiciene.

I takt med at teknologien fortsætter med at udvikle sig, vil IT-sikkerhed og ISO 27001 i hjemmet kræve konstant opmærksomhed og justeringer. Det er vigtigt at være opmærksom på nye trusler, teknologier og sikkerhedsstandarder og tage proaktive skridt for at beskytte sig mod potentielle angreb og sikre et sikkert digitalt miljø i hjemmet og på arbejdspladsen.

## 5.9 UDVIKLING AF EN MINIFICERET VERSION AF ISO27001 TIL HJEMMET

ISO 27001 Mini for hjemmet: En tilpasset vejledning til informationssikkerhed for hjemmebrugere

- Anvendelse af en risikobaseret tilgang: Identificer og vurder potentielle trusler og risici for informationssikkerhed i hjemmet. Prioriter risici baseret på sandsynlighed og indvirkning og implementer passende kontrolforanstaltninger for at reducere eller eliminere disse risici.
- Udvikling af en informationssikkerhedspolitik: Formuler en enkel, men omfattende informationssikkerhedspolitik, der dækker grundlæggende principper og retningslinjer for sikker brug af IT-systemer og -enheder i hjemmet.
- Adgangskontrol: Implementer adgangskontrolforanstaltninger, såsom unikke bruger-id'er og stærke adgangskoder, for at sikre, at kun autoriserede personer har adgang til følsomme data og systemer.
- Sikkerhedsopdateringer og patch management: Opdater regelmæssigt software, operativsystemer og firmware på IT-enheder for at beskytte mod kendte sårbarheder og trusler. Hold øje med sikkerhedsopdateringer og patches fra producenter og leverandører.
- Sikker kommunikation og datatransmission: Brug kryptering og sikre kommunikationsprotokoller for at beskytte data, der sendes og modtages over netværk, herunder Wi-Fi og internetforbindelser.
- Sikker opbevaring af data: Anvend passende sikkerhedsforanstaltninger, såsom kryptering og sikkerhedskopiering, for at beskytte vigtige og følsomme data mod tab, lækage og uautoriseret adgang.
- Fysisk sikkerhed: Sikre, at IT-systemer og -enheder er beskyttet mod uautoriseret adgang, tyveri og skader fra miljømæssige faktorer, såsom brand, vand og strømafbrydelser.
- Bevidstgørelse og uddannelse: Uddan og oplys husstandens medlemmer om informationssikkerhed og god praksis for at minimere menneskelige fejl og sikre et konstant højt niveau af beskyttelse.
- Overvågning og revision: Overvåg regelmæssigt IT-systemer og -enheder for at identificere eventuelle sikkerhedsbrister og hændelser. Gennemfør periodiske revisioner af informationssikkerhedsprocesserne for at sikre deres fortsatte effektivitet og relevans.
- Kontinuerlig forbedring: Evaluer og opdater informationssikkerhedsprocesser og -foranstaltninger løbende for at imødegå ændringer i trusselsbilledet, teknologiske fremskridt og husstandens behov.

Ved at følge denne mini-version af ISO 27001, der er tilpasset til hjemmet, kan hjemmebrugere skabe et mere sikkert og beskyttet miljø for deres IT-systemer og -enheder. Denne tilgang tager højde for de unikke udfordringer og behov, som hjemmebrugere står overfor, og tilbyder en praktisk og forståelig ramme for at forbedre informationssikkerheden. Ved at implementere disse principper og processer vil hjemmebrugere kunne reducere risikoen for sikkerhedshændelser, såsom hacking, datamisbrug og sikkerhedsbrister, og dermed beskytte deres personlige data og digitale ressourcer. Samtidig vil denne tilpassede version af ISO 27001 hjælpe med at skabe en sikkerhedskultur i hjemmet, der fremmer ansvarlighed, opmærksomhed og kontinuerlig forbedring af informationssikkerhedspraksis.

- Identifikation af IT-sikkerhedstrusler og -sårbarheder i hjemmet, herunder enheder, software og data
- Udvikling af en IT-sikkerhedspolitik og procedurer for hjemmet, der omfatter krav til passwords, netværkssikkerhed, adgangskontrol og sikkerhedskopiering
- Implementering af sikkerhedsstyring i hjemmet, herunder overvågning af IT-sikkerhedsrisici og håndtering af trusler og sårbarheder
- Uddannelse og opbygning af bevidsthed om IT-sikkerhed i hjemmet, inklusive træningsmaterialer og information om de udviklede sikkerhedsprocedurer
- Opfølgning på sikkerhedsprocedurer og retningslinjer for IT-sikkerhed i hjemmet, inklusive regelmæssig opdatering og revision af procedurerne.

### 5.9.1 EKSEMPEL PÅ RENSKREVET PLAN FOR EN RISIKOBASERET TILGANG

Eksempel på en informationssikkerhedsplan for en husstand med to voksne, hvoraf den ene arbejder for virksomheden ACME A/S, og to børn på henholdsvis 14 og voksne på 19 år. Planen er baseret på de råd, der er givet tidligere og skal være enkel og indeholde tilstrækkelig information til at passe til et hjem.

- Risikobaseret tilgang:
    - Identificer trusler og risici forbundet med virksomhedsdata, personlige enheder og online-aktiviteter for alle familiemedlemmer.
    - Prioriter risici baseret på sandsynlighed og indvirkning, og fokuser på at implementere kontrolforanstaltninger for de højeste prioriterede risici.
- Informationssikkerhedspolitik:
    - Formuler en enkel og omfattende politik, der dækker principper og retningslinjer for sikker brug af IT-systemer og enheder for alle familiemedlemmer, herunder arbejdsrelaterede og personlige enheder.
- Adgangskontrol:
    - Opret unikke bruger-id'er og stærke adgangskoder for alle familiemedlemmer.
    - Sikre, at arbejdsrelaterede data og systemer kun er tilgængelige for den voksne medarbejder i ACME A/S.
- Sikkerhedsopdateringer og patch management:
    - Opdater regelmæssigt software, operativsystemer og firmware på alle enheder, herunder computere, smartphones og IoT-enheder.
    - Abonner på opdateringsmeddelelser fra producenter og leverandører.
- Sikker kommunikation og datatransmission:
    - Brug kryptering og sikre kommunikationsprotokoller for alle enheder og netværksforbindelser.
    - Undervis familiemedlemmer i sikker brug af e-mail, chat og sociale medier.
- Sikker opbevaring af data:
    - Krypter følsomme data, både arbejdsrelaterede og personlige.
    - Sikkerhedskopier vigtige filer regelmæssigt og opbevar dem sikkert.
- Fysisk sikkerhed:

    - Placer IT-systemer og enheder sikkert for at forhindre uautoriseret adgang og beskytte mod miljømæssige risici.
    - Overvej at bruge en låsbar skuffe eller et skab til opbevaring af bærbare computere og andre værdifulde enheder.
- Bevidstgørelse og uddannelse:
    - Uddan alle familiemedlemmer i informationssikkerhed og god praksis, herunder sikker browsing, adgangskodehåndtering og beskyttelse af privatlivets fred.
    - Opdater uddannelsen regelmæssigt for at imødegå nye trusler og teknologiske ændringer.
- Overvågning og revision:
    - Overvåg IT-systemer og enheder for at identificere eventuelle sikkerhedsbrister og hændelser.
    - Gennemfør periodiske revisioner af informationssikkerhedsprocesserne for at sikre deres fortsatte effektivitet og relevans.
- Kontinuerlig forbedring:
    - Evaluer og opdater informationssikkerhedsprocesser og foranstaltninger løbende for at imødegå ændringer i trusselsbilledet, teknologiske fremskridt og husstandens behov.
- Børns online-sikkerhed:
    - Vejled og overvåg børnenes online-aktiviteter for at sikre, at de forstår og følger sikkerhedsprincipperne.
    - Installer forældrekontrolsoftware på enheder, som børnene bruger, for at begrænse adgangen til upassende indhold og beskytte deres privatliv og sikkerhed.
- Håndtering af sikkerhedshændelser:
    - Udarbejd en handlingsplan for håndtering af sikkerhedshændelser, der dækker trin for at identificere, rapportere og løse hændelser.
    - Gennemgå handlingsplanen med alle familiemedlemmer, så de er bekendt med den og ved, hvad de skal gøre i tilfælde af en sikkerhedshændelse.
- Samarbejde med ACME A/S:
    - Følg virksomhedens retningslinjer for informationssikkerhed og arbejde hjemmefra.
    - Kommunikation med virksomhedens IT-afdeling for at holde dem opdateret om eventuelle sikkerhedshændelser eller bekymringer kan være gavnligt. Dette kan også hjælpe med at indhente råd om effektiv beskyttelse af virksomhedsdata og systemer i hjemmet.

Ved at følge denne informationssikkerhedsplan kan husstanden opretholde et højt niveau af beskyttelse for både arbejdsrelaterede og personlige data og enheder. Planen skal gennemgås og opdateres regelmæssigt for at imødegå ændringer i trusselsbilledet, teknologiske fremskridt og familiens behov.

## 5.10 HVAD ER MEST REALISTISK AT FORVENTE IFT. HJEMMESIKKERHEDEN

Mange mennesker ønsker at beskytte deres hjem og ejendele, men de mangler ofte den tekniske viden, der er nødvendig for at gøre det effektivt. Det er værd at overveje, at en almindelig tendens blandt mennesker er at tilsidesætte betydningen af sikkerhed og vælge lette adgangskoder, hvilket kan gøre deres hjem mere sårbare over for indbrud og andre trusler.
For dem uden teknisk indsigt, kan det være realistisk at tænke på at tage nogle grundlæggende forholdsregler for at forbedre hjemmesikkerheden. Disse kan omfatte:

- At låse døre og vinduer, når de forlader hjemmet eller går i seng.
- At installere god belysning omkring hjemmet for at kunne afskrække potentielle indbrudstyve.
- At overveje at anskaffe en simpel alarm eller overvågningssystem, der kan advare dem, hvis der er en indtrængen.

- At bruge stærke og unikke adgangskoder til alle online konti og enheder, der er tilsluttet hjemmet, såsom smarte låse og overvågningskameraer.

I det lange løb kan det være realistisk at forestille sig, at teknologiske fremskridt og øget bevidsthed om sikkerhed kan føre til bedre sikkerhedsløsninger for hjemmet. Dette kan indebære smartere og mere integrerede sikkerhedssystemer, der er lette at bruge og forstå for folk uden teknisk ekspertise. Derudover kan uddannelse og oplysning om vigtigheden af sikkerhed og gode adgangskodevaner potentielt bidrage til at øge sikkerheden i hjemmet.

For at arbejde hen imod et højere niveau af hjemmesikkerhed, kan det være vigtigt for folk uden teknisk indsigt at søge rådgivning fra professionelle og holde sig informeret om nye teknologier og trusler. Dette kan hjælpe dem med at vurdere de mest effektive sikkerhedsforanstaltninger for deres hjem og arbejde hen imod at beskytte sig selv og deres ejendele både nu og i fremtiden.

Det er dog værd at bemærke, at nogle grundlæggende principper for informationssikkerhed fra ISO 27001 kan anvendes på hjemmesikkerhed. Almindelige mennesker kan lære fra disse principper og anvende passende foranstaltninger for at beskytte deres personlige data og digitale enheder. For eksempel:

- Risikovurdering: At forstå de potentielle trusler og sårbarheder, der er forbundet med deres digitale liv, og træffe informerede beslutninger om, hvilke sikkerhedsforanstaltninger der skal implementeres.
- Adgangskontrol: At sikre, at adgangen til personlige data og enheder kun gives til dem, der har brug for det, og at stærke adgangskoder og autentificeringsmetoder anvendes.
- Overvågning og revision: At holde styr på, hvem der har adgang til hvilke oplysninger og enheder, samt at gennemgå disse oplysninger regelmæssigt for at identificere og løse potentielle problemer.
- Uddannelse og bevidsthed: At lære om informationssikkerhed og opbygge en kultur, hvor familie og venner er opmærksomme på de potentielle risici og træffer foranstaltninger for at minimere dem.

Selvom det kan være urealistisk at forvente, at almindelige mennesker fuldt ud implementerer en standard som ISO 27001 i deres hjem, kan de drage fordel af nogle af de grundlæggende principper og praksisser for at forbedre deres digitale sikkerhed og beskytte deres personlige oplysninger.

## 5.11 IMPLEMENTERING AF GRUNDLÆGGENDE IT SIKKERHED

Dette afsnit bygger på den velinformerede vejledning fra SikkerDigital.dk og suppleres med ekspertise inden for forsyningssektorens cybersikkerheds-strategier fra Dubex og CSIS. Fokus er på implementering af disse anbefalinger på en effektiv måde, både i erhvervsmæssige og private sammenhænge. Rådene spænder fra grundlæggende praksis, såsom opdatering af programmer og anvendelse af stærke adgangskoder, til mere avancerede strategier, der involverer segmenteret adgangskontrol og leverandørsikkerhed. Med en klar fremstilling af disse aspekter af IT-sikkerhed er dette afsnit designet til at ruste læseren til at navigere sikkert i den digitale verden.

Valget af de to tekster giver et perspektiv på den nuværende praksis inden for cybersikkerhed. På den ene side viser de 7 råd fra SikkerDigital.dk de overordnede best practices, der kan anvendes af både organisationer og enkeltpersoner. På den anden side giver de 10 råd fra Dubex og CSIS et eksempel på specifikke sikkerhedstiltag, der er rettet mod et bestemt industriområde, nemlig forsyningssektoren. Imidlertid kan det stadig være en udfordring for private personer at forstå og implementere disse

anbefalinger på en effektiv måde, hvilket understreger behovet for enklere og mere brugervenlige løsninger.

## 5.12 DE 7 GODE RÅD TIL IT-SIKKERHED FRA SIKKERDIGITAL.DK

De syv sikkerhedsråd fra SikkerDigital.dk [24] er relevante, idet de tilbyder praktisk og omfattende vejledning i at beskytte digitale liv for både virksomheder og enkeltpersoner. Ved at efterleve disse grundlæggende og effektive praksisser er det muligt at nedbringe risikoen for cyberangreb og sikre fortrolighed, integritet og tilgængelighed af kritiske data og systemer. I en verden, hvor digitale trusler konstant udvikler sig, er det essentielt at være proaktiv og implementere disse anbefalede sikkerhedsforanstaltninger for at opretholde et sikkert og pålideligt digitalt miljø.

Disse råd omfatter:

- **Få overblik over vigtige data og systemer**: Det er vigtigt at identificere, hvilke data og systemer der er mest kritiske for en virksomhed eller det personlige liv. Ved at opnå en klar forståelse af, hvad der skal beskyttes, kan sikkerhedsforanstaltninger prioriteres, og risici minimeres.
- **Opdater programmer løbende:** Sørg for at installere de seneste opdateringer til dine softwareprogrammer og operativsystemer. Opdateringer indeholder ofte sikkerhedsrettelser, der beskytter mod kendte sårbarheder og trusler.
- **Køb antivirus og firewall:** Invester i et pålideligt antivirusprogram og en firewall for at beskytte dine enheder mod malware, vira og uautoriseret adgang. Disse værktøjer fungerer som en første forsvarslinje mod cybertrusler.
- **Tag backup af data:** Lav regelmæssige sikkerhedskopier af dine vigtige filer, både personlige og arbejdsrelaterede. Opbevar sikkerhedskopierne på et sikkert sted, såsom en ekstern harddisk eller en skytjeneste, for at kunne gendanne dine data i tilfælde af et cyberangreb eller teknisk fejl.
- **Lær at spotte mistænkelige mails:** Vær opmærksom på phishing-angreb og lær at genkende mistænkelige e-mails, der forsøger at få dig til at oplyse personlige oplysninger eller klikke på skadelige links. Tjek afsenderens e-mailadresse og undgå at interagere med mistænkelige indhold.
- **Lav stærke adgangskoder og brug to-faktor login:** Brug komplekse adgangskoder, der indeholder en blanding af bogstaver, tal og specialtegn. Anvend forskellige adgangskoder for forskellige konti, og skift dem regelmæssigt. Aktivér to-faktorautentificering, hvor det er muligt, for at øge sikkerheden.
- **Stil sikkerhedskrav til IT-leverandøren:** Ved samarbejde med en IT-leverandør er det vigtigt at sikre overholdelse af høje sikkerhedsstandarder for effektiv beskyttelse af data og systemer. Det er afgørende at kræve, at leverandøren implementerer passende sikkerhedsforanstaltninger og forbliver opdateret om de nyeste trusler.

Ved at følge de syv sikkerhedsråd fra SikkerDigital.dk kan IT-sikkerheden styrkes og risikoen for at blive ramt af cyberkriminalitet minimeres. Dette bidrager til beskyttelsen af data, systemer og enheder.

Det er plausibelt, at de syv råd fra SikkerDigital.dk kan udgøre en tilstrækkelig grundlag for at etablere en sikker hjemmearbejdsplads. I denne sammenhæng er det imidlertid vigtigt at tage højde for de varierende beskæftigelsestyper, som individer kan have, og som hver især stiller specifikke krav til sikkerhedsforanstaltninger. F.eks. kan en stilling som softwareudvikler kræve en mere robust VPN-forbindelse, mens en stilling som telefonsælger kan stille andre krav til sikkerheden. Ved at følge de syv råd fra SikkerDigital.dk vil der være en øget fokus på sikkerhed, hvilket med høj sandsynlighed vil resultere i en forbedret og bredere forståelse af sikkerhedsproblematikker både i hjemmet og på arbejdspladsen.

## 5.13 DE 10 GODE RÅD TIL IT-SIKKERHED FRA DUBEX OF CSIS

Cybersikkerheds-rådgivning for vand- og spildevandsselskaber DANSKVAND [25] har henvendt sig til to it-sikkerhedseksperter med specifik indsigt i forsyningssektoren for at indsamle anbefalinger til, hvordan vand- og spildevandsselskaber bedst kan beskytte sig mod cyberkriminelle trusler.
Peter Kruse, en it-sikkerhedsekspert og partner i CSIS Security Group [26], og Jacob Herbst, Chief Technology Officer i Dubex [27], repræsenterer begge virksomheder, der er anerkendt inden for cybersikkerheds-branchen. Kruse og Herbst besidder dybdegående viden om de specifikke udfordringer og forhold, der er forbundet med forsyningsselskaber.
DANSKVAND har anmodet Peter Kruse, it-sikkerhedsekspert og partner i CSIS Security Group, samt Jacob Herbst, Chief Technology Officer i Dubex, om at bidrage med deres ekspertise. Disse to virksomheder er førende inden for cybersikkerhed og har en omfattende forståelse for de unikke forhold, der kendetegner forsyningssektoren.

1. Ledelsesmæssig prioritering af cybersikkerhed For at opnå effektiv cybersikkerhed skal ledelsen prioritere de mest betydningsfulde sikkerhedsudfordringer og virksomhedens ansvar. Den indledende fase indebærer udarbejdelse af en risikovurdering, der fungerer som et prioriteringsværktøj, hvilket kan hjælpe med at identificere områder, der kræver øjeblikkelig opmærksomhed og allokerede ressourcer.
2. Implementering af segmenteret adgangskontrol En systematisk opdeling af adgangsrettighederne for brugere til forskellige oplysninger og operationer bør gennemføres. Brugeradgang bør begrænses til det absolut nødvendige, og en segmenteringsstrategi bør anvendes for at minimere risiciene forbundet med uautoriseret adgang.
3. Leverandørers cybersikkerhed Segmentering er særlig vigtig, når partnere eller leverandører kræver adgang til systemer. Det er essentielt at reducere angrebsfladen og kontrollere cybersikkerheds-niveauet hos partnere og leverandører, herunder skytjenester.
4. Kontinuerlig opdatering af software Regelmæssige sikkerhedsopdateringer af software er afgørende for at undgå sårbarheder, der kan udnyttes af cyberkriminelle.
5. Robuste adgangskoder og to-faktor-godkendelse er ofte et svagt punkt i cybersikkerhed. Implementering af to-faktor-godkendelse tilføjer et ekstra lag af beskyttelse og bør overvejes som en nødvendighed.
6. Medarbejderuddannelse i cybersikkerheds-bevidsthed Uddannelse af medarbejdere i cybersikkerheds-bevidsthed kan hjælpe med at forhindre dem i at falde for forsøg på manipulation og svindel, såsom phishing.
7. Digital overvågning og logning Indførelse af digital overvågning på operationel teknologi kan hjælpe med at spore uregelmæssigheder og forsøg på indtrængen i systemet. Logning kan give realtidsadvarsler og støtte i effektiv efterforskning af sikkerhedshændelser.
8. Beredskabsplanlægning og penetrationstest Udarbejdelse af en beredskabsplan er vigtig for at sikre, at medarbejdere ved, hvordan de skal reagere i tilfælde af en sikkerhedshændelse. Planen bør regelmæssigt opdateres og testes. Penetrationstest, hvor et hold af etiske hackere forsøger at finde sårbarheder i sikkerheden, kan også være en værdifuld tilføjelse til beredskabsplanen.
9. Fysisk adgangskontrol Fysisk adgangskontrol og sikkerhedsprocedurer er afgørende for at beskytte forsyningens infrastruktur og udstyr mod uautoriseret adgang og potentielle digitale angreb. Dette er særlig relevant inden for vandsektoren, hvor beskyttelse af bygninger, anlæg og udstyr skal prioriteres.
10. Sikkerhedskopiering og datagendannelse At have en pålidelig og testet it-sikkerhedskopi er vigtig for at sikre kontinuiteten af systemet i tilfælde af uoprettelige forstyrrelser som følge af et cyberangreb. Det er afgørende at teste sikkerhedskopierne for at validere deres evne til at reetablere systemet effektivt og rettidigt.

Disse 10 råd fremsætter en grundig og praktisk vejledning til implementering af robuste IT-sikkerhedsløsninger inden for vand- og spildevandsselskaber. De understreger behovet for omfattende

forholdsregler, som spænder fra ledelsesmæssige prioriteringer til fysiske adgangskontroller og datasikkerhedsbackups. Selvom disse retningslinjer er rettet mod en bestemt sektor, fremhæver de overordnede principper, der er relevante for alle virksomheder, der ønsker at forbedre deres cybersikkerhed. Udfordringerne ved at implementere sådanne strategier er betydelige, men de potentielle konsekvenser af at ignorere IT-sikkerhedsrisici er langt større. Det er derfor afgørende, at alle virksomheder og private personer tager aktive skridt for at styrke deres cybersikkerheds-procedurer.

## 5.14 DELKONKLUSION

I denne delkonklusion samles de vigtigste pointer og indsigter fra teksten om IT-sikkerhed og implementering af ISO 27001 i hjemmet. Det er blevet belyst, at IT-sikkerhed i hjemmet er en afgørende faktor, der skal tages alvorligt, idet der er forskellige risikofaktorer, der kan påvirke sikkerheden. Normale sikkerhedsforanstaltninger såsom opdatering af software og enheder, stærke adgangskoder og to-faktor-autentifikation er nødvendige for at beskytte hjemmets IT-systemer.

IoT-enheder i hjemmet udgør en særlig sikkerhedsudfordring, og der er blevet identificeret forskellige trusler og sårbarheder samt sikkerhedstiltag, der kan beskytte disse enheder. ISO 27001, en international standard for sikkerhedsledelse, er blevet præsenteret som en mulig løsning til at øge IT-sikkerheden i hjemmet, selvom implementeringen kan være udfordrende og kræve en simplificeret version af standarden, der er tilpasset hjemmets behov. Bevidsthed og uddannelse om IT-sikkerhed og ISO 27001 er nødvendige for at skabe en sikker kultur i hjemmet og forebygge trusler.

Fremtidige udviklinger inden for IT-sikkerhed og ISO 27001 i hjemmet vil kræve tilpasning til nye teknologier og trends samt en generel forventning om en højere grad af hjemmesikkerhed. Ydermere er gode råd til IT-sikkerhed fra sikkerdigital.dk og Dubex og CSIS præsenteret, hvilket underbygger vigtigheden af proaktivt at tage hånd om IT-sikkerheden i hjemmet.

Sammenfattende understreger denne tekst vigtigheden af IT-sikkerhed i hjemmet og værdien af at overveje implementering af ISO 27001 samt nødvendigheden af bevidsthed og uddannelse om IT-sikkerhed for at skabe et sikkert hjemmemiljø.

# 6 KONKLUSION

Denne rapport har undersøgt, hvordan IoT-enheder i danske hjem kan udgøre en trussel mod IT-sikkerheden, og rapporten har identificeret konkrete løsninger for at sikre disse enheder. Trusler fra IoT-enheder inkluderer muligheden for, at cyberkriminelle kan få adgang til følsomme oplysninger, hvilket kan føre til identitetstyveri, økonomisk svindel og andre former for misbrug. En standardiseret sikkerhedsstandard for IoT-enheder er nødvendig for at højne sikkerhedsniveauet og mindske risiciene forbundet med IoT-enheder i danske hjem.

For at sikre IoT-enheder i danske hjem er det vigtigt at fokusere på konkrete løsninger. Dette inkluderer øget fokus på uddannelse og bevidsthed om IT-sikkerhed, forbedring af IoT-arkitektur, softwareopdateringer samt anvendelse af stærke adgangskoder og to-faktor-autentificering. For at skabe et mere specifikt billede af, hvordan disse løsninger kan implementeres i praksis, kunne en IoT-enhed udvælges, og der kunne redegøres for, hvordan denne enhed kan sikres.

Sikring af IT-sikkerhed er en kompleks opgave, som kan være udfordrende for den gennemsnitlige bruger. Det kræver en teknisk opgradering af brugerens viden om IT-sikkerhed, og kommunikationen omkring sikkerhed bør være letforståelig og tilgængelig for alle. Dette vil bidrage til at mindske risiciene for brud på IT-sikkerheden og skabe en mere sikker IT-infrastruktur for både brugere og organisationer. Uddannelse og øget bevidsthed om IT-sikkerhed er nødvendige for at sikre IoT-enheder i danske hjem, og det er afgørende at have fokus på konkrete løsninger. Forbedring af IoT-arkitektur, softwareopdateringer, stærke adgangskoder og to-faktor-autentificering er blot nogle af de mulige tiltag. Det er også vigtigt at standardisere sikkerhedsstandarderne for IoT-enheder, da dette vil bidrage til at øge sikkerhedsniveauet og gøre det nemmere for brugere at vælge sikre enheder. Samtidig er det afgørende at anvende flere kilder, herunder ekspertudsagn og praktikeres erfaringer, for at opnå en nuanceret forståelse af problemstillingen.

Standardisering af sikkerhedsstandarder er også vigtigt for at øge sikkerheden i IoT-enheder og netværk. En standardiseret sikkerhedsstandard kan hjælpe med at sikre, at IoT-enheder opfylder minimumskrav til sikkerhed og kan gøre det nemmere for brugere at vælge sikre enheder. Det er vigtigt at anvende flere kilder for at opnå en nuanceret forståelse af problemstillingen. Udover litteraturgennemgangen kan ekspertudsagn og erfaringer fra praktikere på området også give et bredere perspektiv.
Et brud på IT-sikkerheden kan have alvorlige konsekvenser, både for enkeltpersoner og organisationer. Hvis en persons personlige oplysninger, såsom kreditkortoplysninger eller adgangskoder, bliver kompromitteret, kan det føre til identitetstyveri, økonomisk svindel eller anden form for misbrug af oplysningerne. Hvis en organisation bliver hacket, kan det føre til datatab, finansielle tab eller en negativ påvirkning af omdømmet. Desuden kan brud på IT-sikkerheden også give cyberkriminelle adgang til fortrolige eller følsomme oplysninger, såsom personlige sundhedsoplysninger eller militære hemmeligheder, som kan have alvorlige konsekvenser.

Selvom sikring af IT-sikkerhed kan være en udfordring for mange brugere, er det vigtigt at fortsætte med at udvikle effektive løsninger og skabe en sikker IT-infrastruktur i danske hjem. Dette vil medvirke til at mindske truslerne fra IoT-enheder og styrke IT-sikkerheden generelt. Endelig skal forskning inden for IoT-enheder og IT-sikkerhed fortsætte, da dette er et stadigt udviklende område med stadig nye udfordringer og risici, som skal tackles.

# 7 REFLEKSION

I løbet af projektet stødte jeg på udfordringer med at finde relevante kilder til mit litteratur review. Det var ikke selve søgningen på databaserne, der var problemet, men snarere at finde forskning, der specifikt omhandlede hjemmets sikkerhed på den måde, som min problemformulering var udformet. Selvom jeg overvejede at ændre problemformuleringen, besluttede jeg at holde fast i den og søge videre for at finde den mest effektive metode, der kunne give de bedste søgeresultater.

Under min søgen var jeg klar over, at ny forskning potentielt kunne blive offentliggjort undervejs i projektet eller efter, at jeg var færdig med at skrive. Jeg overvejede at inddrage denne nye forskning, men valgte i sidste ende at holde mig til de udvalgte artikler, da jeg vurderede, at den nye forskning sandsynligvis ville bekræfte det eksisterende materiale.

Gennem dette projekt har jeg lært meget om at læse forskningsartikler, og det har givet mig et nyt perspektiv på, hvordan jeg kan inddrage relevant viden i min egen undervisning. At få en god start på projektet har været en udfordring, men jeg har givet mig selv de bedste forudsætninger for at komme i gang. Den største udfordring har været, at jeg ikke er akademisk skolet, hvilket har betydet, at jeg har skullet læse en del tekster og gennemgå samtaler for at finde frem til den rette struktur og skrivestil. Dette har dog været en lærerig proces, og jeg er taknemmelig for muligheden og de nye færdigheder, jeg har opnået.

De resultater, jeg fandt i forskningen, overraskede mig ikke: generelt mangler folk evnerne til at skabe bedre IT-sikkerhed i hjemmet eller på arbejdspladsen. I mit daglige arbejde som underviser ser jeg denne tendens blandt mine kolleger, der har meget forskellige uddannelsesbaggrunde. Selv noget så simpelt som at identificere front-end og back-end på en hjemmeside kan være udfordrende, da vi ikke alle taler det samme tekniske sprog og uddannelsesretningerne bruger forskellige terminologier.

# 8 CITEREDE VÆRKER


[1] »version2,« https://digi.no/, 8 Marts 2019. [Online]. Available: https://www.version2.dk/artikel/iot-nogle-enheder-er-saa-usikre-det-ikke-kan-skyldes-en-fejl.

[2] A. Tystrup, »Flere arbejder hjemme,« 24 februar 2010. [Online]. Available: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/bagtal/2010/2010-02-24-Hjemmearbejde.

[3] W. T. Jensen, »Hjemmearbejde fordoblet i 2020,« 23 februar 2021. [Online]. Available: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=32435.

[4] A. Tassy og M. B. Nielsen, »Europarekord i brug af 'smart home'-produkter,« 3 marts 2020. [Online]. Available: https://www.dst.dk/Site/Dst/Udgivelser/nyt/GetPdf.aspx?cid=36216.

[5] A. Brinck, »https://www.computerworld.dk,« Computerworld, 11 september 2020. [Online]. Available: https://www.computerworld.dk/art/279193/50-procent-stigning-det-smarte-hjem-er-under-angreb.

[6] A. Brinck, »50 procent stigning: Det smarte hjem er under angreb,« 11 September 2020. [Online]. Available: https://www.altomdata.dk/hackerangreb-paa-iot-i-smarte-hjem/.

[7] A. Brinck, »100.000 kontoransatte danskere er blevet hacket – installerer opdateringer for sent,« 02 December 2021. [Online]. Available: https://www.altomdata.dk/100-000-kontoransatte-hacker-aod-pro/.

[8] »Fjernarbejde har sendt ansvaret for sikkerhed over på medarbejderne,« 18 Februar 2022. [Online]. Available: https://www.altomdata.dk/it-sikkerhed-paa-hjemmekontoret-aod-pro/.

[9] X. Feng, X. Zhu, Q. -L. Han, W. Zhou, S. Wen og Y. Xiang, »Detecting Vulnerability on IoT Device Firmware: A Survey,« *IEEE/CAA Journal of Automatica Sinica,* årg. 10, nr. 1, pp. 25-41, 2023 https://doi-org.zorac.aub.aau.dk/10.1109/JAS.2022.105860.

[10] B. D. Davis, J. C. Mason og M. Anwar, »Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study,« *IEEE Internet of Things Journal,* årg. 7, nr. 10, pp. 10102-10110, 2020 https://doi-org.zorac.aub.aau.dk/10.1109/JIOT.2020.2983983.

[11] B. Zhao, S. Ji, M. I. W.-H. Lee, C. Lin, H. Weng, J. Wu, P. Zhou, S. Member, L. Fang og R. Beyah, »A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices,« *IEEE Transactions on Dependable and Secure Computing,* årg. 19, nr. 3, pp. 1826-1840, 2022 https://doi-org.zorac.aub.aau.dk/10.1109/TDSC.2020.3037908.

[12] R. M. Abdulghani, M. M. Alrehili, A. A. Almuhanna og O. H. Alhazmi, »Vulnerabilities and Security Issues in IoT Protocols,« *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH),Riyadh, Saudi Arabia,* pp. 7-12, 2020 https://doi-org.zorac.aub.aau.dk/10.1109/SMART-TECH49988.2020.00020.

[13] M. Lalit, S. K. Chawla, A. K. Rana, K. Nisar, T. R. Soomro og M. A. Khan, »IoT Networks: Security Vulnerabilities of Application Layer Protocols,« *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS),* pp. 1-5, 2022 https://doi-org.zorac.aub.aau.dk/10.1109/MACS56771.2022.10022971.

[14] V. Chalasani og W. Alhamdani, »A Survey on the Security Vulnerabilities of IoT Smart Home Application,« *2021 IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT),* pp. 114-121, 2021 https://doi-org.zorac.aub.aau.dk/10.1109/ICISSGT52025.2021.00030.

[15] E. Ahmed, A. Islam, M. Ashraf, A. I. Chowdhury og M. M. Rahman, »Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider,« *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India,* pp. 1-6, 2020 https://doi-org.zorac.aub.aau.dk/10.1109/ICCCNT49239.2020.9225283.

[16] B. Nazzal, A. A. Zaid, M. H. Alalfi og A. Valani, »Vulnerability Classification of Consumer-based IoT Software,« *2022 IEEE/ACM 4th International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT), Pittsburgh, PA, USA,* pp. 17-24, 2022 https://doi-org.zorac.aub.aau.dk/10.1145/3528227.3528566.

[17] »ISO/IEC 27001:2022,« International Organization for Standardization, [Online]. Available: https://www.iso.org/standard/82875.html. [Senest hentet eller vist den 2023].

[18] »NIST National Institute of Standards and Technoloy,« 2023. [Online]. Available: https://www.nist.gov/cyberframework.

[19] »Enisa,« The European Union Agency for Cybersecurity (ENISA), 2023. [Online]. Available: https://www.enisa.europa.eu/.

[20] »Komputer,« Bonnier Publications International AS, 2 Marts 2018. [Online]. Available: https://komputer.dk/it-og-samfund/smart-home/styr-dit-hjem-med-stemmen.

[21] S. D. »Sikker Digital,« Digitaliseringsstyrelsen, [Online]. Available: https://sikkerdigital.dk/virksomhed/beskyt-virksomheden/iot-beskyt-virksomhedens-internet-forbundne-enheder.

[22] »Danskindustri,« Danskindustri, [Online]. Available: https://www.danskindustri.dk/vi-radgiver-dig/forretningsudvikling/digitalisering-og-innovation/grib-nye-teknologier/iot/.

[23] »CISA - Cybersecurity & Infrastructure Security Agency,« CISA, [Online]. Available: https://www.cisa.gov/news-events/news/securing-wireless-networks.

[24] »sikkerdigital.dk,« Digitaliseringsstyrelsen, 2023. [Online]. Available: https://sikkerdigital.dk/virksomhed/syv-raad-om-it-sikkerhed.

[25] »Dansk Vand,« DANVA Dansk Vand- og Spildevandsforening, 2023. [Online]. Available: https://www.danva.dk/.

[26] »CSIS,« CSIS Security Group A/S, 2023. [Online]. Available: https://csis.com/.

[27] »Dubex,« Dubex A/S, 2023. [Online]. Available: https://www.dubex.dk/.

[28] »Hjemmearbejde mest udbredt i Danmark,« 27 juli 2011. [Online]. Available: https://www.dst.dk/pukora/epub/Nyt/2011/NR342.pdf.

[29] »NordVPN,« 2023. [Online]. Available: https://nordvpn.com/.

[30] »Expressvpn,« 2023. [Online]. Available: https://www.expressvpn.com/.

[31] »Wirelesslogic,« Wireless Logic, [Online]. Available: https://www.wirelesslogic.com/da/case-study/energyteam/.