MALMÖ UNIVERSITET

Det digitala hemmet & säkerhetssystemet

Möjligheter och utmaningar

The digital home & security system

Opportunities and challenges

Beatrice Göransson

Yahya Ahmad

IT och Ekonomi
Kandidatuppsats
13 HP
VT 23
Handledare: Dipak Surie

DET DIGITALA HEMMET & SÄKERHETSSYSTEMET

Kandidatuppsats

Göransson, Beatrice, It och ekonomiprogrammet, Malmö Universitet, Sverige

Ahmad, Yahya, It och ekonomiprogrammet, Malmö Universitet, Sverige

Abstrakt

Tillkomsten av digital teknik har lett till betydande framsteg i olika aspekter av våra liv, inklusive konceptet smarta hem. Ett smart hem är en innovativ integration av sammankopplade enheter och system som syftar till att förbättra komfort, bekvämlighet och säkerhet i bostadsmiljöer. Detta examensarbete utforskar möjligheter och utmaningar förknippade med det digitala smarta hemmet, med ett specifikt fokus på dess säkerhetssystem. Huvudsyftet med denna studie är att analysera de potentiella fördelar och möjligheter som uppstår genom att implementera ett digitalt säkerhetssystem. Den fördjupar sig i de tekniska framstegen som möjliggör automatisering, energieffektivitet och förbättrad livskvalitet för husägare. Men i takt med att hem blir allt mer digitaliserade ökar också sårbarheten för cyberattacker och integritetsintrång. Därför syftar denna forskning till att identifiera säkerhetsrisker och sårbarheter som är ett resultat av den sammankopplade naturen hos smarta hemenheter. Den undersöker de åtgärder och strategier som kan användas för att skydda smarta husägares integritet, dataintegritet och personlig säkerhet. Genom att genomföra en omfattande litteraturgenomgång och expertintervjuer ger denna uppsats en djupgående analys av de möjligheter och utmaningar som det digitala smarta hemmet och säkerhetssystemet utgör. Resultaten bidrar till en omfattande förståelse av de tekniska framstegen inom detta område och belyser deras konsekvenser för husägare, branschfolk och beslutsfattare. I slutändan fungerar den här avhandlingen som en värdefull resurs för individer och organisationer som vill dra nytta av de möjligheter som digitala smarta hem erbjuder samtidigt som de effektivt tar itu med de associerade utmaningarna. Det ger insikter i bästa praxis för att säkra smarta hemsystem och understryker vikten av att utveckla robusta säkerhetsprotokoll för att skydda husägares integritet och tillgångar i en allt mer sammankopplad värld.

Nyckelord: IoT, digitala säkerhetssystem, smarta hem, integritet, möjligheter och utmaningar.

Abstract

The advent of digital technologies has brought forth significant advancements in various aspects of our lives, including the concept of a smart home. A smart home is an innovative integration of interconnected devices and systems that aim to enhance comfort, convenience, and security within a residential setting. This thesis explores the opportunities and challenges associated with the digital smart home, more specifically its security system. The primary objective of this study is to analyze the potential benefits and opportunities that arise from the implementation of a digital security system. It delves into the various technological advancements that enable automation, energy efficiency, and improved quality of life for homeowners. As the digitalization of homes advances, the vulnerability to cyber-attacks and privacy breaches increases. This research aims to identify potential security risks and vulnerabilities that arise from the interconnected nature of smart home devices. It investigates the measures and strategies that can be employed to safeguard the privacy, data integrity, and personal security of smart homeowners. Through a combination of literature review and expert interviews, this thesis provides an in-depth analysis of the opportunities and challenges posed by the digital smart home and security system. The findings of this research contribute to a comprehensive understanding of the technological advancements in the field and shed light on the implications for homeowners, industry professionals, and policymakers. Ultimately, this thesis serves as a valuable resource for individuals and organizations seeking to leverage the opportunities presented by digital smart homes while addressing the associated challenges. It offers insights into best practices for securing smart home systems and underscores the importance of developing robust security protocols to protect homeowners' privacy and assets in an increasingly interconnected world.

Keywords: IoT, digital securitysystems, smart homes, integrity, possibilities and challenges.

1 Inledning

Teknikens utveckling i samhället de senaste decennierna har medfört flera industriella revolutioner (Teknikföretagen, 2021). Det förklaras att teknikutvecklingen i Sverige går så långt tillbaka som 1800-talet. Alltifrån dess har tekniken tagit sig an flertalet former som drivit fram nya möjligheter och utmaningar inom den digitala världen. Däremot har den digitala utvecklingen sedan 2000-talet nått nya höjder. Den har fört fram tekniker som Artificiell Intelligens, IoT, Bioteknik, Big Data, 3D- printing med mera (Teknikföretagen, 2021). De nya digitala teknikerna som oftast är plattform- och nätverksbaserade har påverkat samt till en stor del förändrat det vardagliga livet för den individuella människan men även för den organisatoriska världen, detta innefattar även alla olika verksamheter som exempelvis sjukvården, e-handel, skolor och liknande (Forskning, 2016).

Denna nya digitala utveckling och allt den tillbringar benämns idag som den fjärde industriella revolutionen eller Industri 4.0, en revolution som producerat enorm digital utveckling. Den har lyckats infiltrera människors privatliv i så stor utsträckning att den har fått fotfäste i hemmet. Detta görs främst idag via IoT, vilket står för “Internet of Things” (Gravina m.fl., 2017). Internet of Things innefattar ett nätverk av fysiska enheter som besitter sensorer, kameror, mikrofoner, högtalare, programvaror och anslutningar. Det som gör dessa enheter speciella är att de kan samla in och utbyta data mellan varandra och ägaren via användning av internet. IoT drivs fram av automatisering samt digital transformation och den sträcker sig från komplexa industrisystem till autonoma fordon, men i detta arbete är de smarta hemmen i fokus. I dagens samhälle är människan starkt beroende av tekniken till den grad att det är vanligt att IoT finns i de flesta hemmen. Att ha digitala artefakter hemma som är uppkopplade till ett gemensamt nätverk och kan kommunicera med varandra går idag under namnet "smarta hem”.

Ett smart hem är ett koncept som förenklar användarens liv, vilket den gör genom att ägna sig åt erfarenhet av individers behov och sedan anpassa sig därefter (IOT Sverige, u.å.). Syftet med smarta hem är att tillhandahålla tjänster som bättre säkerhet, hemunderhållning, som att tända eller släcka lampor och sätta igång musik, och kontroll av energi, temperatur, brandlarm och säkerhetskameror. Den är utformad för att minska den mänskliga involveringen vid driften av manuella hem och ge användarna möjligheten att samla information och tjänster med hjälp av det smarta hemmet. Det är känt för att förenkla vardagen för användaren och bistå med ett lugn och bekvämlighet genom att användaren får ett stöd med informerade val och ett stöd i beslutsfattande genom att systemet tillhandahåller dem med viktig information om hushållet. Det förklaras även att smarta hem ska inom framtiden kunna tillbringa tjänster inom medicin, säkerhet, underhållning och kommunikation (Balakrishnan, m.fl. 2018). Balakrishnan m.fl. (2018) skriver vidare om vilka fördelar och möjligheter som de smarta hemmen kan ge användarna, där de smarta hemmer erbjuder oändliga möjligheter att introducera smarta enheter som kan kopplas ihop och kontrolleras på avstånd. En av många möjligheter de presenterar är hur de smarta hemmen skapar ett allt större intresse för enheter inom energisparande, där fokuset ligger på att minska energisvinnet genom en grön energikälla som bidrar till en bättre miljö genom naturliga kyl- och värmesystem, vattenbesparing samt soldrivna vitvaror. Författarna lyfter fram att

möjligheterna är många där dessa går från sjukhusutrustning i hemmen till bättre miljö till bättre livskvalitet i olika slag (Balakrishnan, m.fl. 2018).

Eftersom ett smart hem är uppkopplat till nätverk kan data enkelt extraheras av externa parter och användas i multipla syften utan användarens kännedom eller insyn. En sådan situation sker enkelt idag på grund av att användare tvingas godkänna långa licensavtal innan användning där inte allt framgår särskilt tydligt.

1.1 Problembakgrund

1.1.1 Möjligheter

Miller (2015) hävdar att IoT är ett växande fenomen genom att den förväntas överträffa det internet vi känner till idag i form av storlek, betydelse samt intäkter. Vidare förklaras det att Vinnova, svenska verket för innovationssystem, uppskattat att det fanns 50 miljarder uppkopplade enheter i världen år 2020. Enligt statistik utdragen från Statista (2023) uppskattas intäkterna för smarta uppnå 135,90 miljarder euro år 2023. Vidare förklaras det att den årliga tillväxten beräknas uppgå till 11,86%, vilket i sin tur resulterar i en marknadsvolym på 212,80 miljarder euro år 2027. Dessutom att antalet smarta hem förväntas uppnå 672,6 miljoner världen runt år 2027.

Saizmaa (2008) förklarar att hemmet fungerar som en gräns mellan samhället och den privata sfären. Vidare berättar de att människor som använder sig av IoT i de smarta hemmen oftast inte är oroliga för dataintrång eller integritetskränkning utan att de tänker mest på personskador som exempelvis brand. Detta då hemmet är en trygg och privat plats som finns för människans bekvämlighet och avslappning. En stor del av Saizmaas (2008) forskning visar att användning av IoT-enheter bidrar till bekvämlighet, energisparande, hållbarhet samt säkerhet. Säkerhet i form av att det konstant finns kameraövervakning, dörrarna är låsta samt att brandlarm slår om något händer.

1.1.2 Utmaningar

Som tidigare förklarat består det smarta hemmet av ett antal uppkopplade digitala enheter. Detta nätverkssystem använder sig av molntjänster för att lagra sin information (Microsoft Azure u.å.). Detta är i princip ett måste för att smarta hem ska fungera optimalt. Det vill säga den behöver ständigt samla in känslig information om användaren för att kunna fungera som bäst. Men hur vet en digital artefakt om hur mycket data som är tillräcklig för att utföra tjänsten och när överskrider den gränsen för integritetsintrång? Dessutom ökar detta risken för integritetskränkning ifall obehöriga lyckas åstadkomma denna lagrade information i molntjänster.

Saizmaa (2008) förklarar att även om syftet med smarta hem är att effektivisera och underlätta för användaren så måste det ske på ett sätt där individens säkerhet samt integritet inte äventyras. Detta är ett problem då Mansfield-Devine (2016) understryker att

IoT-enheterna inte är så säkra i sig. Det vill säga att leverantörer inte sätter tillräckligt mycket fokus på att bilda enheterna så säkert som möjligt. Detta upplevs problematiskt då cyberattacker eller hackning är vanligt i dagens samhälle (Östlund, 2021).

Petersson & Sördal (2018) förklarar att säkerhet i form av den personliga integriteten fortfarande är ett färskt ämne men att detta ämne har blivit alltmer välkänt och utforskat ända sedan skandalen kring Facebook och Cambridge Analytica. Det förklaras även att trots lagar och regler så lyckas vi inte riktigt skydda den personliga integriteten. Det vill säga att den enkelt äventyras.

Brown & Adams (2007) lyfter i sin artikel att studier fokuserar mer på de smarta enheternas möjlighet till datainsamling än enheternas etiska gränser. Författaren menar att enheterna inte enbart representerar en teknisk utmaning utan även en etisk utmaning. Där de etiska analyserna av de smarta enheterna väcker en oro om förlusten av integritet, social isolering och samtycke. Trots att det smarta hemmet bidrar till människans bekvämlighet menar han på att individer är villiga att offra sin integritet för att slippa det traditionella säkerhetssystemet. Vidare poängterar Sfar m.fl. (2018) att det är av större vikt att lyfta fram etiken bakom integritet inom IoT då informationssäkerheten är begränsad eller inte särskilt effektiv. Där de smarta hemmen kan hamna i konflikt med de sociala skyldigheter som ett företag besitter genom ta hänsyn till deras kunders isolering, följden av detta kan bli att kunderna väljer att inte använda sig av smarta hem då känslan av att alltid bli avlyssnad eller sedd tar övertaget.

1.1.3 GDPR

När GDPR introducerades tvingades många leverantörer av IoT att kolla igenom sina processer. Dessa nya regler har haft stor påverkan på hur produkter, processer och lösningar har designats. Enheter som är uppkopplade i exempelvis smarta hem är produkter som skulle kunna vara enklare för hackare att komma åt. Numera måste intrång på system som behandlar personuppgifter anmälas om det skulle kunna vara av risk för individers frihet eller rättigheter. En annan regel är samtycke, IoT-lösningar fångar upp en del data som tillhör individerna, dessa nämns numera som personuppgifter och kräver att personen i fråga ska informeras om vad det är för data som samlas in (IDG Expert Network, 2018). Anders Englund (IDG Expert Network, 2018) menar vidare att GDPR skapat ett ansvar där produkter behöver ha grundläggande organisatoriska och tekniska lösningar där det finns ett krav på privacy by design (dataskydd). Om produkten inte lever upp till detta krav kommer leverantören att stå som ansvarig i det fall att information skulle läckas ut på grund av underhåll eller konstruktion av produkten. För att undvika detta kan företagen granska säkerheten i deras enheter men också i hela systemet, vilket borde göras löpande och inte bara under tillverkning och utveckling. Till sist lyfter dessa reglerna de rättigheter som individerna har, rätten att få veta vilken information som finns sparad, rätten att föra vidare datan till något annat företag, rätten att glömmas bort samt rätten att neka automatiserade beslut (IDG Expert Network, 2018).

1.1.4 Integritet

Statistiska centralbyrån genomförde år 2006 en enkätundersökning där de ville ta reda på allmänhetens syn på om den personliga integriteten inkräktas av kameraövervakning. 97% av deltagarna ansåg att så länge kameraövervakning används i syftet att förebygga brott så hade de en positiv inställning (Marklund och Tollin, 2020). Författarna Marklund och Tollin (2020) skriver vidare att undersökningar har gjorts vid flera tillfällen av datainspektionen för att ställa frågan om kameraövervakning och integritet till yngre människor mellan 15 och 18 år. Där visade de en större acceptans för kameraövervakning med brottsbekämpning som syfte till skillnad från att vara kontrollerad via internet som enligt denna åldersgrupp anses som kränkande mot deras integritet. Vidare skriver de att procentsatsen var 85% bland ungdomarna som hade en acceptans för övervakningskameror om syftet är att minska brottsligheten.

En liknande undersökning gjordes på ekonomihögskolan vid Lunds Universitet där resultatet var överensstämmande med de undersökningar som gjordes av Statistiska centralbyrån och Datainspektionen. De som hade en positiv inställning till kameraövervakning uppgick till 90%, denna siffran minskade med 15% när frågan om de anser att deras personliga integritet blev påverkad då 75% inte tyckte att deras personliga integritet blev påverkad när det kom till allmänna platser. Ännu lägre blev procentsatsen när frågan riktade sig till bostadsområden då enbart 66% ansåg att kamerorna inte var integritetskränkande (Marklund och Tollin, 2020).

1.2 Leverantör

Den valda leverantören har 4,7 miljoner kunder och har etablerat sig i 17 länder inom Europa och Latinamerika vilket gör dem till en ledande leverantör inom professionellt övervakade larm. Affärsmodellen som företaget skapat innefattar design, produktutveckling, försäljning och service, som alla tas fram i deras Innovation Center i två stora städer. De har utvecklat en plattform för framtiden som kan erbjuda deras kunder ett originellt sortiment av tjänster och produkter inom det uppkopplade smarta hemmet. Med sina 30 år i branschen har de även fått uppleva uppmärksammade blåsväder.

2022 publicerades en granskning av 200 sekunder där det visat sig att oberättigade bilder på kunder cirkulerat hos de anställda. De flesta gångerna utlöstes larmet och tog bilderna på personerna som nyligen vaknat ur sömn eller lämnat duschen när deras respektive larmat trots att de var hemma, där bilderna sedan spreds blixtsnabbt mellan de anställda (Norrgrann m.fl, 2022).

I granskningen har det även framkommit att larmen varit felinstallerade och trillat ner från väggarna och i värsta fall har inbrott gjorts utan att larmet utlöst trots att de boende larmat när de gått hemifrån. Det visade sig då att larmen inte fungerade vart 5:e gång. Inte heller skickade de ut räddningstjänst på grund av för få kameror och rökdetektorer vilket enligt 200 sekunder berodde på att de anställda fick provision när de undvek att skicka väktare (Aschberg & Mohlin, 2022).

1.3 Problematisering

Det digitala hemmet har som syfte att underlätta vardagen för hushållen genom att flera funktioner automatiseras och interagerar med varandra via ett nätverk, vilket innebär att hushållens privata information måste lagras på internet (Al-Fuqaha m.fl. 2015). Genom att ständigt behöva vara uppkopplad för att hålla hushållet säkert utgör inte bara en utan flera risker, dels är det enklare för obehöriga att komma åt andras information och dels så är det även en risk om systemet skulle krascha (Alaba m.fl. 2017). Det är många som undersöker i sina rapporter om risker och utmaningar samt om hur säkert det egentligen är för individen. Denna studie kommer därför att rikta sig till de möjligheter och utmaningar som kommer med det digitala hemmet och säkerhetssystem ur ett användarperspektiv. Med tanke på dess relativt snabba intåg på marknaden skulle det även kunna klassas som en trend inom hushållen där man kan känna sig mer avslappnad och säker, men hur stora är utmaningarna när det kommer till den personliga integritet eller när nätverkssystemet och molntjänsterna inte fungerar som dem ska. Och hur stora är möjligheterna för användarna gällande hållbarhet, säkerhet och bekvämlighet. De områden som kräver vidare forskning och som är av större relevans inom området är därmed att se på möjligheter och utmaningar genom användarens perspektiv.

Då de smarta hemmen kan innehålla flera olika enheter har vi i detta arbete valt att fokusera på det säkerhetssystem som det leverantören har utvecklat för sina kunder där de kan styra sitt hem via deras app. Företagets app är en IT-lösning som underlättar för användarna att styra hemmet oavsett var de befinner sig genom att sammankoppla olika lösningar på en plattform. Lösningar som att larma på och av på distans, styra över lampor, klimat, kameror och annan elektronik samt att kolla om dörrar eller fönster står öppna är några av de funktioner som användarna får åtkomst till via appen. Med tanke på företagets etablering på marknaden som en av de ledande leverantörerna av säkerhetssystem kommer detta arbete att använda denna leverantör som exempel och hjälpmedel för att studera vilka möjligheter och utmaningar som finns med digitala säkerhetssystem. Leverantören har trots sin framgångsrika etablering upplevt diverse blåsväder under sina många år i branschen, vilket skulle kunna ge en differentierad inblick i vilka utmaningar och möjligheter som kan uppstå med säkerhetssystem i digitala hem. Som tillverkare har de även möjlighet att ge ett perspektiv på vad de smarta enheterna kan bidra med gällande möjligheter och utmaningar.

Genom att applicera detta fokus i studien skapas möjligheten att ta reda på vad det är som gynnar användarna när de använder sig av smarta hem, vidare kan vi ta reda på hur mycket kunskap användarna anses behöva för att systemet ska kunna hålla dem trygga för att till sist knyta ihop säcken med hjälp av leverantörens perspektiv och hur dem arbetar med för att leverera det bästa systemet till sina kunder. Vidare kan det studeras om systemet har en viss påverkan på användarna, hur upplever de sin integritet och säkerhet genom appen. Denna inriktning kan ge studien ett bredare perspektiv på hur utmaningar och möjligheter kan uppstå genom information från både företaget och användarna samtidigt som etiken lyfts fram från båda dessa parter. Arbetets resultat skulle därmed kunna lyfta vilka viktiga aspekter som leder

till möjligheter eller utmaningar som kan bidra till smarta enheters design och tillverkning inom smarta hem.

1.4 Syfte och frågeställning

Syftet med denna uppsats är att skapa en större kunskap om hur användare och leverantören upplever användningen av det digitala säkerhetssystemet i smarta hem. Smarta hem och digitala säkerhetssystem blir allt mer populärt att forska om med tiden som det blir allt mer vanligt i alla hem, det är många som lyfter vilka risker och säkerhetsaspekter som dessa medför. Uppsatsen tar därför stöd i användarperspektivet genom att undersöka hur användarna påverkas av systemet men även hur leverantören tänker kring systemet som levereras till användarna. Frågeställningen som ska besvaras för att släta ut glappet inom forskningen är därmed följande:

- Hur upplever användare och leverantören användningen av digitala säkerhetssystem i smarta hem?

2 Relaterad forskning

2.1 Digitalisering

Termen "digitalisering" hänvisar till processen att anta och integrera digital teknik, system och praxis i olika aspekter av samhället, organisationer eller industrier (Gray & Rumpe, 2017). Digitalisering innebär omvandling av analog information, processer och tjänster till digitala format, vilket gör dem mer tillgängliga, effektiva och kompatibla med digitala system (Digitaliseringskommissionen, 2016). Det omfattar användningen av digital teknik som datorer, internet, mjukvaruapplikationer och dataanalys för att effektivisera verksamheten, förbättra kommunikationen, öka produktiviteten och möjliggöra innovation.

2.2 Internet of Things

Internet of Things, IoT, ett bredare begrepp som hänvisar till nätverket av fysiska enheter, fordon, apparater och andra objekt inbäddade med sensorer, mjukvara och anslutningsmöjligheter för att utbyta data över internet (IOT Sverige, u.å.). Dessa enheter, ofta kallade "smarta" eller "anslutna" enheter, kan samla in och överföra data, interagera med andra enheter eller system och utföra olika funktioner utan mänsklig inblandning. I ett smart hem är IoT-enheter de komponenter som möjliggör sammankoppling och kommunikation mellan olika enheter i hemmet.

IoT-konceptet kretsar kring idén att ansluta vardagliga föremål till internet, så att de kan kommunicera, dela data och fjärrstyras eller övervakas. Miller (2015) förklarar att dessa objekt kan sträcka sig från små, enkla enheter som sensorer eller ställdon till komplexa system som smarta hem, smarta städer eller industrimaskiner. IoT-enheter är vanligtvis

utrustade med sensorer för att samla in data om sin omgivning eller specifika parametrar. De använder denna data för att utföra specifika funktioner eller utlösa åtgärder. Till exempel kan en smart termostat i ett hem känna av temperaturen och justera den automatiskt baserat på fördefinierade inställningar. På samma sätt kan en bärbar tränings-spårare samla in data om en persons aktivitetsnivåer och överföra den till en mobilapp för analys och spårning (Miller, 2015).

Miller (2015) förklarar att IoT-enheter förlitar sig på anslutningstekniker som Wi-Fi, Bluetooth, cellulära nätverk eller Low-Power Wide-Area Networks (LPWAN) för att upprätta kommunikation och överföra data. Den insamlade informationen skickas ofta till molnet eller lokala servrar för lagring, bearbetning och analys. Avancerad teknik som dataanalys, artificiell intelligens och maskininlärning kan användas för att få insikter, göra förutsägelser och automatisera åtgärder baserat på insamlad data. Tillämpningarna av IoT är omfattande och varierande, allt från smarta hem, smarta städer, industriell automation, jordbruk, sjukvård, transporter och mer (Mansfield-Devine, 2016). IoT har potential att revolutionera olika branscher genom att möjliggöra förbättrad effektivitet, automatisering, realtidsövervakning, förbättrat beslutsfattande och nya affärsmodeller.

2.3 Smarta Hem

Bugeja, m.fl. (2016) förklarar att ett smart hem hänvisar till en bostad utrustad med sammankopplade enheter och system som kan styras och automatiseras för att förbättra bekvämlighet, komfort, säkerhet och energieffektivitet. Termen "smart" i smarta hem indikerar integrering av digital teknik och anslutning för att möjliggöra centraliserad styrning och automatisering av olika funktioner i hemmiljön (Balakrishnan, m.fl. 2018). Dessa enheter, ofta kallade smarta enheter eller Internet of Things (IoT)-enheter, använder en kombination av sensorer, ställdon och anslutningstekniker som Wi-Fi, Bluetooth eller Zigbee för att möjliggöra kommunikation och interaktion mellan enheter. Vanliga exempel på smarta enheter som finns i ett smart hem är:

- Smart belysning: Belysningsarmaturer och glödlampor som kan fjärrstyras, dämpas eller programmeras för att skapa önskade ljusscener.
- Smarta termostater: HVAC-system (värme, ventilation och luftkonditionering) som kan fjärr-justeras, lära sig användar-preferenser och automatiskt optimera energianvändningen.
- Smarta säkerhetssystem: Säkerhetskameror, dörrlås, rörelsesensorer och larmsystem som kan övervakas och kontrolleras var som helst för att förbättra säkerheten i ett hem.
- Smarta apparater: Hushållsapparater som kylskåp, tvättmaskiner och ugnar som kan styras, övervakas och programmeras för energieffektivitet och bekvämlighet.

- Smarta underhållningssystem: Ljud- och video-enheter, inklusive smarta TV-apparater, högtalare och streaming-enheter, som kan integreras och styras för personliga underhållningsupplevelser.

- Smarta hem-assistenter: Röstaktiverade virtuella assistenter som Amazons Alexa, Google Assistant eller Apple Siri som kan utföra olika uppgifter och interagera med andra smarta enheter genom röstkommandon.

- Smart energihantering: Energiövervakningssystem som ger realtids insikter om energiförbrukning, som hjälper husägare att fatta välgrundade beslut för att minska energislöseriet och spara kostnader.

Det här är bara några exempel på det breda utbudet av smarta enheter som finns tillgängliga för att skapa ett smart hem. Integreringen och automatiseringen av dessa enheter gör det möjligt för boende att kontrollera och hantera olika aspekter av sin hemmiljö, vilket ökar komforten, bekvämligheten och effektiviteten (Bugeja, m.fl. 2016). Det är värt att notera att termen "smart hem" ofta används omväxlande med termer som "uppkopplat hem" eller "hemautomation." Även om dessa termer delar likheter, hänvisar de i allmänhet till samma koncept att använda teknik för att skapa ett intelligent och sammankopplat boende.

2.4 CIA

Carlsson & Jacobsson (2012) skriver om tre centrala begrepp som tillsammans bildar begreppet CIA, Konfidentialitet (Confidentiality) - Okränkbarhet (Integrity) - Tillgängligt (Availability). Dessa tre begreppen bildar tillsammans målet med informationssäkerhet, det som man vill uppnå med implementering av skyddsmekanismer är att skydda någon eller något från skada. Genom att använda sig av dessa tre begrepp som kompletterar varandra, kan ett system bedömas som säkert.

Författarna (Carlsson & Jacobsson, 2012) beskriver att innebörden med konfidentialitet är att obehöriga inte ska ha tillgång till informationen, användaren ska bestämma vem som ska få ta del av den och begreppet har i vår forskning en stark koppling till personlig integritet. Vidare beskriver de att begreppet okränkbart innebär att informationen får enbart ändras på godkända sätt, alltså att information inte får modifieras eller ändras utan användarens godkännande. Till sist skriver författarna (Carlsson & Jacobsson, 2012) om tillgänglighet, att informationen ska hela tiden finnas tillgänglig för de behöriga användarna, begreppet innebär att förebygga att information undanhålls.

2.5 RITE

RITE står för Ansvar (Responsibility) - Integritet (Integrity) - Förtroende (Trust) och Etik (Ethicality) och skulle enligt Kajtazi (2013) kunna ses som ett komplement till CIA principen. Rite fungerar som en grundsats för strategisk informationssäkerhet vilket har lett till ett ökat behov av att studera beteendet hos de anställda. Denna princip innehar en sådan

möjlighet att kunna mäta egenskaper för efterlevnad och bristande efterlevnad av informationssäkerhetsprogrammet inom organisationen (Kajtazi, 2013). Vidare skriver Kajtazi (2013) att informationssäkerhet grundar sig i de påtagliga elementen, säkerhetsteknik, samt de immateriella elementen, medvetenhetsprogram. Tidigare har de påtagliga elementen ansetts vara en framgångsrik policy inom informationssäkerhet men numera har de immateriella elementen som kan kopplas till RITE principerna varit nyckeln till framgångsrik informationssäkerhet (Kajtazi, 2013).

2.6 Teknikens påverkan på individen

Verbeek (2011) anser att möjligheter till svar på problem som skulle kunna förhindra en produkt öppnas upp genom att ställa frågan: "Hur är ett bra sätt att leva med denna teknik?". Med detta menar författaren att konsekvenserna får en tydligare relevans genom att teknik och etik inte står som motståndare till varandra. Tekniken bör ses från ett perspektiv där den inte är en inkräktare som kräver etiska gränser i individernas liv, den teknik som inte anses självklar i samhället bör istället granskas för att sedan avgöra om den kommer att bidra med något positivt eller negativt i våra liv. Verbeek (2011) menar på att teknik och produkter inte kan utvecklas utan någon som helst effekt på samhället och användarna.

Verbeek & Tijink (2020) skriver att teknologi och människor är som "två partners i en dans", där de förknippas med varandra och har en kontinuerlig påverkan på varandra. Guidance Ethics Approach skiljer sig från andra etiska förhållningssätt genom att den inte utgår från människans bedömning av teknikens utveckling, detta förhållningssätt riktar sig till interaktionen och hur frågan: "hur kan människor och teknik utvecklas på ett värdefullt sätt?" istället för ja eller nej frågan. Vidare skriver Verbeek & Tijink (2020) att många etiska resonemang lägger fokus på teknikens eventuella nackdelar, men deras perspektiv lägger fokus på teknikens både negativa och positiva delar, där författarna betonar vikten av att båda sidorna behöver utrymme i en dialog.

Teknikens roll i det vardagliga livet behöver enligt Verbeek (2011) en tydligare bild för att vi ska kunna utvärdera om det är rätt eller fel i det moraliska perspektivet. Fokuset bör vara på huruvida det finns någon påverkan på livet och hur det är att leva med den nya tekniken istället för att stirra oss blinda på det etiska perspektivet. Ett viktigt krav som ställs på tekniken är att de som använder sig av tekniken ska kunna känna sig trygga vid användandet, med detta menas att det ska finnas en tillit till användningsområdet och möjliga risker som kan resultera i negativa påföljder för användaren samt att användandet av tekniken inte ska kunna användas emot användarna (Verbeek, 2011).

3 Metod

I metodkapitlet nedan beskriver vi studiens genomförande. Det tydliggörs hur vi gått tillväga samt arbetat för att uppnå bästa möjliga resultat. Därtill redogörs hur arbetets forskning har skett samt vilka tillvägagångssätt vi valt för att lyckas leverera faktiska och relevanta resultat.

Dessutom följer en noggrann beskrivning om datainsamlingen och hur det genomförts via litteratur, forskning samt intervjuer.

3.1 Studiedesign

3.1.1 Forskningsstrategi

Kvalitativ forskning
Den huvudsakliga forskningsfrågan för denna studie är, "Hur upplever användare och leverantören användningen av digitala säkerhetssystem i smarta hem?". För att besvara denna forskningsfråga har vi genomfört en kvalitativ studie som inkluderar både primära och sekundära analys- och datainsamlingsmetoder. Det vill säga att genomföra en litteraturgenomgång för att identifiera befintlig forskning om möjligheter och utmaningar med digitala säkerhetssystem i smarta hem. Därtill genomfördes kvalitativa intervjuer med användare och leverantörer av smarta hemsystem för att samla information om det aktuella tillståndet för digitala säkerhetssystem i smarta hem, inklusive möjligheter och utmaningar. Intervjuerna har genomförts antingen personligen eller på distans med hjälp av digitala verktyg och har spelats in för transkription och analys. Därefter använde vi oss av multipla tekniker för att analysera data och innehåll vi erhållit via intervjuer och litteraturforskning. Detta gjordes i hopp om att identifiera gemensamma teman och mönster.

Sammantaget beskriver denna forskningsstrategi ett riktat tillvägagångssätt för att studera möjligheter och utmaningar med digitala säkerhetssystem i smarta hem. Genom att samla in insikter från olika intressenter och analysera sekundära datakällor hoppades vi kunna ge värdefulla insikter och rekommendationer till husägare och säkerhetsleverantörer som vill förbättra den digitala säkerheten och därmed de digitala säkerhetssystemen i smarta hem.

Hermeneutik
Forskningen har ett hermeneutiskt synsätt som utgångspunkt, hermeneutiken syftar till hur insamlat material tolkas, det vill säga att forskarens förståelse eller fördomar kan speglas i hur denna person tolkar det material som samlats in (Thurén, 2007). Jürgen Habermas och den kritiska hermeneutiken (Hallberg, 1978) menar på att forskaren behöver exponera underliggande mekanismer som skulle kunna förvrida en formulering eller upplevelse och hur dessa framställs enskilt men också mot reella egenskaper, därför sattes kriterier för den kvalitativa forskningen upp i arbetet som gjorde det möjligt att se skillnad på förståelse och missförståelse. Detta hermeneutiska synsätt användes vid genomförande av intervjuer samt vid transkriberingen av intervjuerna och användes därmed som en andrahandsanalys.

Deduktiv ansats
En deduktiv ansats syftar till att forskarens arbetssätt utgår ifrån befintliga teorier och allmänna teorier för att därmed kunna dra slutsatser av den data som samlats in. Patel och Davidson (2003) menar på att objektiviteten i forskningen blir starkare genom att den deduktiva ansatsen grundar sig i befintlig teori. Forskaren bevisar hypoteser med hjälp av etablerade principer för att sedan empiriskt testa dem samt undersöka hur de stämmer överens med verkligheten. Studien grundades därmed på en deduktiv forskningsansats då frågorna

kom att formas med hjälp av teorier om modeller om säkerhet i digitala hem. Den deduktiva ansatsen användes som primär analys genom arbetets gång.

3.1.2 Datainsamling

Arbetet byggdes främst på semistrukturerade intervjuer som metod där tre av åtta intervjuer utfördes med hjälp av anställda som arbetar med digitala säkerhetssystem hos den valda leverantören och resterande intervjuer utfördes med hjälp av fem hushåll som använder sig av deras digitala säkerhetssystem. Denscombe (2018) förklarar att denna metod, till skillnad från strukturerade intervjuer, möjliggör mer flexibla och öppna intervjuer där intervjupersonen enkelt kan utveckla och lägga till svar. Det vill säga att man enkelt kan få ut en mängd information ur intervjupersonen, exempelvis med hjälp av följdfrågor som en semistrukturerad intervju möjliggör. Denna metod var viktig för detta arbete då vi intervjuade användare samt företag och ville ställa frågor som berörde olika områden. Med hjälp av en semistrukturerad intervju kan man anpassa sig och ställa specifika följdfrågor beroende på respons inom ett visst intressant område eller ett område man kräver mer information kring. Detta till skillnad från andra metoder där strukturerade intervjuer enbart bygger på tidigare bestämda frågor och de ostrukturerade intervjuerna bygger på att personen som blir intervjuad pratar fritt och den personen som intervjuar interagerar så lite som möjligt (Oates, 2006). Semistrukturerade intervjuer användes i denna studie för att kunna skapa ett mer spontant och personligt tillvägagångssätt samtidigt som den semistrukturerade intervjun kunde säkerställa en mer objektiv sammanställning av informationen från samtliga personer som blev intervjuade. Vidare byggde detta arbetet på kvalitativa data som samlades in via litteraturkällor som nyhetsartiklar och vetenskapliga artiklar. Dessa källor hämtades från Malmö Universitets bibliotek, Malmö universitets elektroniska databas, DiVA-portal, Google Scholar samt IEEE Explorer.

3.1.3 Val av respondenter

Då arbetet utgår ifrån en kvalitativ metod är genomförandet av intervjuer av relevans för att samla in den data och förståelse för hur användare och företag resonerar kring den frågeställning som besvaras i detta arbete. Intervjuerna delades upp i två grupper, där den ena gruppen var användare av digitala säkerhetssystem som dagligen använde sig av dessa system. Den andra gruppen var personer som arbetade på ett av Europas främsta företag inom säkerhet där de arbetade som bland annat produktchef eller servicetekniker/installatör.

3.1.4 Val av intervjufrågor

Syftet med arbetet var att besvara forskningsfrågan där upplevelse av användning med säkerhetssystem är i fokus ur ett leverantör- samt användarperspektiv, för att skapa en större förståelse och bredare kunskap har intervjuerna riktat sig till både användare och företag. Intervjufrågorna som formulerades blev därför uppdelade i två sektioner, där tjugo stycken förberedda frågor om användandet av systemet, integritet och säkerhet ställdes till

användarna och fjorton stycken förberedda frågor om säkerhet, möjligheter och utmaningar med systemet ställdes till de anställda på det valda företaget. Utöver dessa frågor ledde dialoger vidare till följdfrågor som skrevs ner under intervjuernas gång för att skapa en större förståelse där det behövdes eller för vidareutveckling av intervjun. Då dessa två grupper kom att intervjuas från två olika perspektiv hade olika frågor för varje grupp formulerats för bästa resultat. Frågorna presenteras i bilagorna ett och två.

3.1.5 Analysmetod

Datamaterialet för denna studie samlades in genom kvalitativa intervjuer. Dessa intervjuer spelades in och därefter transkriberades för att läsas igenom noggrant. Oates m.fl (2022) nämner att analysen av den kvalitativa datan bör förberedas och sorteras för att på enklare sätt filtreras. Vidare nämner författarna vikten av att planera tiden då 1 timmes intervju speglar ca 4-5 timmars transkribering. Det transkriberade materialet godkändes av respondenterna innan användning i arbetet. Analysförfarandet började med att materialet delades upp genom att placeras i olika teman och grupper, där vi använde rubriker som exempelvis möjligheter och utmaningar för att kunna särskilja och mappa ut respondenternas svar. Detta förenklades analysen av datan genom att vi på ett tydligare sätt kunde ställa upp olika tabeller för att kategorisera datan. Dessa teman, grupper och tabeller kan enligt Oates m.fl. (2022) hjälpa till att lokalisera olika data samtidigt som de kan tydliggöra vilken data som fattas.

3.2 Avgränsningar

Detta arbete har till största del grundats med insamlad data från användare och anställda på Europas största leverantör av säkerhetssystem, arbetet är avgränsat till användare och anställda inom Sverige. Majoriteten av intervjuerna gjordes med användarna och resterande gjordes med en junior mjukvaruutvecklare, en installatör/servicetekniker samt en produktchef. Det perspektiv som kom att beaktas var användarperspektivet, detta för att avgränsa det stora området med olika perspektiv som digitala säkerhetssystem erbjuder. Då digitala säkerhetssystem erbjuder många utmaningar men även många möjligheter ansågs det vara relevant att forska ur ett användarperspektiv. Vidare ska det tydliggöras att arbetet inte fokuserar på företaget utan de enheter som de erbjuder sina kunder och användes i syftet att vi som författare kunde begränsa oss till vår frågeställning då ett större område med fler leverantörer hade krävt ett större arbete.

3.3 Forskningsetiska begrundanden

Forskningsetiken i detta arbete har beaktats genom att balansera mellan två intresseområden, kunskap och integritet, i syfte att arbetet ska kunna upprätthålla en aktuell och tidsenlig status. Det har tagits hänsyn till deltagarna genom deras kunskaps- och integritetsintresse, vidare fanns det ett behov av att vi som författare hanterade det material som samlades in på ett korrekt sätt. Kunskapsintresset är av relevans för att forskningen ska få ett adekvat resultat, detta uppnås genom att vända sig till de personer som är erfarna inom området.

Vidare är kunskap av intresse för de som kommer att ta del av denna forskning. Integritetsintresset är av relevans för att inte utsätta deltagarna, användarna eller företag för någon typ av skada. Det är även av stor vikt att deltagarna är medvetna om deras rättigheter både före och under tiden som de var delaktiga i studien.

Enligt Merton har forskaretik fyra grundläggande principer som denna studie utgår ifrån och som utgör "moral consensus". Det handlar om att denna forskning ska finnas tillgänglig för samhället så att de kan ta del av resultatet. Materialet ska utgå ifrån vetenskapliga kriterier med målet att kunna lyfta nya kunskaper. För att detta skulle kunna uppnås fick vi som författare ta del av många olika forskningar, intervjuer och annat material. Detta för att kunna granska och ifrågasätta vad som gäller för vårt intresse för att slutligen kunna ta fram ett resultat som grundar sig i noggrann forskning. Slutligen har vi som författare ett större ansvar att undvika oredlig forskning som fabricering, plagierat eller förfalskning.

3.4 Metoddiskussion

Utmaningar med att intervjua användare
En betydande utmaning som möttes under denna forskning var att rekrytera användare för intervjuer. Det var svårt att övertyga individer att delta i studien, vilket kan ha påverkat urvalsstorleken och potentiellt infört partiskhet. Att utforska alternativa metoder, såsom undersökningar, kan övervägas för att nå en större och mer mångsidig pool av deltagare.

Leverantörens dominans
En annan reflektion avser leverantörens dominans i studien. Även om företaget vi valt gav värdefulla insikter om möjligheter och utmaningar med digitala hem- och säkerhetssystem, kan fokus på ett enda företag begränsa resultatens generaliserbarhet. Att inkludera andra leverantörer och jämföra deras tillvägagångssätt skulle kunna erbjuda ett bredare perspektiv.

Övervägande av forskningsstrategi
I efterhand kunde inkluderingen av undersökningar eller enkäter som en forskningsmetod ha gett ytterligare kvantitativa data för att komplettera de kvalitativa insikterna från intervjuerna. Undersökningar skulle möjliggöra en större urvalsstorlek och möjliggöra statistisk analys för att stödja eller validera resultaten.

4 Empiri

I detta avsnitt presenteras en översikt på de respondenter som deltog i de semistrukturerade intervjuerna. Två tredjedelar av respondenterna använder dig av digitala säkerhetssystem i sina hem och en tredjedel av respondenterna arbetar inom ett företag som levererar digitala säkerhetssystem. Dessa områden bidrar med den kunskap inom det ämne som vi har för avsikt att undersöka. Därefter presenteras resultaten av de semistrukturerade intervjuerna.

Respondent	Yrkesroll	Användare/leverantör	Hur länge de använt/jobbat med systemet	Intervjutyp
1	Lärare	Användare	5 år	Videosamtal
2	Myndighet	Användare	8-10 år	Videosamtal
3	Egen företagare	Användare	15 år	Fysisk
4	Naprapat	Användare	8 år	Videosamtal
5	Företag	Användare	ca. 4 år	Videosamtal
6	Produktchef	Leverantör	3,5 år	Fysisk
7	Junior mjukvarutestare	Leverantör	2 månader	Videosamtal
8	Installatör/Servicetekniker	Leverantör	24 år	Videosamtal

Tabell 1. *Presentation av respondenter som deltog i de semistrukturerade intervjuerna.*

4.1 Användarnas syn på möjligheter med det digitala hemmet och säkerhetssystem

Intervjupersonerna, användare av det digitala säkerhetssystemet, blev tillfrågade hur de påverkats av det digitala säkerhetssystemet och vilka möjligheter detta har skapat. Intervjupersonerna var överens om att det digitala säkerhetssystemet har tillbringat trygghet i deras vardag. Intervjupersonerna förklarar att de är trygga både hemma och när de inte är hemma då det är enkelt att använda det digitala säkerhetssystemet för att kolla hur det ser ut i hemmet. Dessutom förklarar intervjupersonerna att de upplever en större trygghet då man inte behöver tänka så mycket på säkerheten i och med att det digitala säkerhetssystemet varnar om något skulle hända. Därtill berättar intervjuperson 5 att de gånger larmet har utlösts, vilket oftast har varit av misstag, har de fått respons från larmcentralen genom att de ringer upp och kollar vad som sker, vilket i sin tur skapat en känsla av säkerhet hos användarna. Intervjuperson 3 förklarar “Det börjar bli mer och mer viktigt att känna sig säker i dagens samhälle, känner att familjen är tryggare”. Vidare poängterar intervjupersonen att detta är väsentligt att de upplever då det i grund och botten är hela syftet med det digitala säkerhetssystemet.

När intervjupersonerna blev tillfrågade om hur det digitala säkerhetssystemet har påverkat deras vardag och vilka möjligheter det tillbringat har svaren varit väldigt lika. Det användarna uppskattar är att man enkelt kan kolla säkerheten och om larmet är igång. Dessutom att man kan kolla temperatur, batteritid samt vilka kameror som är igång. En viktig funktion för användarna var att man kunde kolla säkerheten hemma även om man var bortrest eller utanför hemmet. Det vill säga att man kan hålla koll på sådant som man vanligtvis inte kan som exempelvis temperaturen, om dörrar och fönster är stängda, om barnen kommit hem, om

man fått sitt paket samt att man kan ta bilder för att kolla läget hemma. Intervjuperson 2 påpekar att de enkelt kan se vem som varit inne i huset, vilket är en stor fördel med det digitala säkerhetssystemet. Därtill berättar intervjuperson 4 “Vi har städning varannan vecka och då har vi även kodlås som är kopplat till larmet och den koden kan vi ju lägga in bara specifika tidpunkter så att dom lätt kommer in i huset och inte kan använda den koden vid andra tillfällen. Vi kan även ha familjemedlemmar med andra koder som gäller antingen hela tiden eller bara om man vill specifikt vissa tider. Så det tyckte vi funka bra med larmet”. Med detta menas att det digitala säkerhetssystemet förändrat användarnas vardag för det bättre och möjliggjort goda vanor för förbättrad säkerhet.

Intervjupersonerna fick svara på frågor om appen och dess användarvänlighet samt vilka möjligheter den tillbringat. Svaren var främst positiva där intervjupersonerna förklarar att appen är lättnavigerad och erbjuder hjälp för användarna. Det vill säga att appen är användarvänlig, smidig och enkel. Intervjuperson 5 påpekar att “mina sidor” på appen eller webbsidan är enkla att använda och det är en stor fördel att man lätt kan skapa behörighet för nya användare. Det vill säga att man enkelt kan ge nya användare tillgång till systemet. Intervjupersonerna berättar även att appen ger möjlighet att se vem som larmat på och av vilket är en viktig grej för ett digitalt säkerhetssystem.

Intervjupersonerna blev tillfrågade om företaget och vad den möjliggjort för att öka deras säkerhet. Intervjuperson 2 påbörjar sitt svar med att säga “Vi är nöjda med allt, vi har även testat larmsystemet själva och det har funkat bra”. Resterande intervjupersoner höll med om att leverantörens fördelar övervinner de negativa delarna. Intervjupersonerna var extra nöjda med den snabba servicen, funktionaliteten och reaktionsförmågan som leverantören erbjöd. Något som nästan alla intervjupersoner var extra nöjda med var att leverantören var snabb och aktivt. Det vill säga att de ringer så fort larmet går samt att de ständigt hjälper till om det skulle ske larm på grund av misstag.

4.2 Leverantörens syn på möjligheter med det digitala hemmet och säkerhetssystem

När frågan om vilka möjligheter som det digitala säkerhetssystemet kan bidra med gentemot användarna ställdes till intervjupersonerna var allas svar enhälligt, de tre personerna nämnde peace of mind som är ett av företagets huvudmål. Möjligheterna som skapas genom att installera ett digitalt säkerhetssystem är att användarna ska känna sig trygga både när de befinner sig i hemmet men även när de är på jobbet eller utomlands. Genom att ha tillgång till en app har användarna ständigt kontroll över appen, de kan exempelvis se till att husdjur är säkra, de kan se när barnen kommer hem samt snabbt få information vid eventuell vattenläcka eller brand, vilket skapar en större trygghet och säkerhetskänsla. Intervjuperson sex och sju som båda jobbar på kontoret nämnde att en trygghetsfaktor är just hur snabb respons som deras larmcentral har till kunderna och SOS om det skulle behövas genom att de har tillgång till alla system när ett larm utlöser. Intervjuperson åtta, som jobbar i fält med försäljning, installation och service, har liknande svar som de andra intervjupersonerna men tillägger att det finns en del franchiseföretagare inom företaget som åker runt i olika distrikt.

Även detta skapar en trygghetskänsla för användarna då de har operatörer som cirkulerar och är tillgängliga i området om något skulle hända med deras digitala säkerhetssystem.

Vid frågan om vilka möjligheter som systemet kan bidra med inom en 5-10 års period gav intervjupersonerna lite olika synvinklar på vad företaget kan komma att erbjuda i framtiden. Intervjuperson sex svarade att de försöker ta sig in på olika marknader och utvidga deras system genom att koppla in flera enheter i det smarta hemmet, till exempel robotdammsugare som har kameror, ljudsystem etcetera. Vidare nämnde personen att deras vision är att ta sig in på nya marknaden, exempelvis introducerade leverantören, Guardian 2020 som är ett personligt skydd kopplat till företagets app och tjänst. Guardian innebär att användare kan vara uppkopplade på systemet så om något skulle hända kan företaget bli informerade och larma vidare.

Intervjuperson sju hade inte varit i företaget under så lång tid och hade därför inte så stor information kring detta men menade på att: “Systemet kommer att bidra med att människor känner sig tryggare i sin vardag, kunder känner att de kan slappna av mer när de inte är hemma” - (Intervjuperson sju).

Intervjuperson åtta informerade om möjligheten att förflytta säkerheten utanför husets väggar där de som har större tomter kan få notiser om någon rör sig på tomten vilket leder till att de snabbare kan förhindra eventuella inbrott. Med detta kan de senare erbjuda fler skräddarsydda lösningar åt användarna. Denna person menade också på att med tiden kan de bygga ännu större förtroende och ett bättre samarbete med SOS genom att se till att larma vid aktiva larm.

4.3 Användarnas syn på utmaningar med det digitala hemmet och säkerhetssystem

Intervjupersonerna frågades om det digitala säkerhetssystemet de använder och vilka utmaningar den tillbringar. Därmed förklarar intervjupersonerna att tänkandet kring säkerheten har förändrats, vilket i sin tur leder till att man blivit mer medveten, spänd och orolig. De påpekar även att det är mycket i systemet som de inte vet hur eller vad man ska använda det till. Intervjupersonerna hade olika perspektiv kring utmaningarna där olika miljöer skapade olika utmaningar. Det vill säga att användare med exempelvis husdjur upplevde problem med att ställa in larm då rörelse triggade igång larmet hela tiden. De förklarar vidare att när man har husdjur hemma kan man enbart ha på skalskydd och inte resten av sitt larmsystem. Därmed får man installera om sitt system så att den är anpassad för husdjur. Intervjupersonerna förklarar att det hade varit till stor hjälp om man kunde larma vissa sektioner. Andra klagade på att priset var ganska högt samt att för varje kamera man väljer att komma åt via appen kostar extra. Intervjuperson 3 berättar att de hört i media att vissa går in och kollar på kamerorna och känner ibland att det kan hända dem själva. Det ovannämnda var användarnas främsta utmaningar när det gäller det vardagliga livet med ett digitalt säkerhetssystem.

Vidare ställdes frågan kring utmaningar med enheterna som intervjupersonerna har hemma och vad som kan förbättras med dem. Multipla intervjupersoner påpekade att man gärna hade

förändrat designen på enheterna samt larmdosan och gjort dem mindre och snyggare. Intervjuperson 4 svarar att hon önskar sig lite nättare produkter så att de kan bli mer enhetliga utseendemässigt. Dessutom förklarar intervjupersonen att de bor ute på åker och ibland kan det komma in djur i enheterna vilket gör att de behöver bytas ibland. Vidare påpekar intervjupersonerna att placeringen på kameror och intervjuer kan förbättras. Detta då vid exempelvis vid städning kan en kamera ändra position vilket resulterar i att larmet inte går att aktivera. Detta upplevs av intervjupersonerna som en stor utmaning då ingen notis kom upp ur systemet utan när de skulle lämna huset gick det inte att slå på larmet. Förbättringen skulle då kunna vara ett tips på hur man ska ställa tillbaka kameran som vid detta fallet var ganska enkelt eller att huset ska kunna gå o larma men att man förlorar kameran tills den är reparerad. En annan stor utmaning var att byta batteri på enheterna. Intervjupersonerna förklarar att enheterna kräver specifika batterier från leverantören själv och att dessa var svåra att få tag på. Därmed måste man ta kontakt med företaget och be om batteribyte vid ett sådant fall.

Slutligen frågades intervjupersonerna om företaget och om de tillbringat några utmaningar. Intervjupersonerna svarade att de var snabba att reagera på larm men långsamma med att svara på mejl och ge feedback. Dessutom att det alltid är telefonkö när man behöver komma åt kundtjänsten. Vidare förklaras det att de är långsamma på mejl och får sällan uppdateringar eller nyheter om det digitala säkerhetssystemet. En annan utmaning som användarna lyfte fram var att de inte fick någon introduktion eller utbildningsfas för användning av appen och säkerhetssystemet. Intervjupersonerna påpekar att de fick lära sig på egen hand och hitta fram samt att de än idag inte vet hur allt funkar. Intervjupersonerna fick även frågan kring inloggning på appen för det digitala säkerhetssystemet där de förklarar att man kommer in direkt utan inloggning. Inloggning av app krävs enbart när telefonen gjort någon uppdatering eller varit avstängd annars är man inloggad hela tiden. Detta upplevs som en utmaning då det skulle vara problematiskt ifall någon obehörig lyckas komma åt appen eller det digitala säkerhetssystemet.

4.4 Leverantörens syn på utmaningar med det digitala hemmet och säkerhetssystem

Vi ställde frågan vilka utmaningar som de kunde finna i det digitala säkerhetssystemet där svaret från intervjuperson sex var att en stor utmaning är att deras kundbas är 55+ vilket gör den digitala biten något svårare, den yngre generationen har lättare att förstå nya enheter och funktioner. De upplever att det är en utmaning att få deras största kundbas att aktivera nya tjänster som introduceras på marknaden. Utmaningar som var kopplade till systemet och appen kändes inte som något större problem då de har tillräckligt stora avdelningar med rätt kompetenser för att hantera eventuella krascher på så kort tid som möjligt. Detta samtidigt som systemen i hemmen inte påverkas om något inte skulle fungera med appen eller om det skulle bli strömavbrott, då alla system har en egen huvudcentral i varje hem.

Intervjuperson sju såg det som en utmaning att resurserna används på rätt sätt, larmen behöver installeras korrekt och operatörerna behöver veta när de ska skicka vakt och polis så

att resurserna inte slösas på falska larm samtidigt som de vill att kunderna ska känna sig trygga med att något faktiskt inte har hänt.

Intervjuperson åtta menade på att en utmaning är att med enkelhet kommer det risker, som installatör informerar de användarna om att inte lämna taggar eller nycklar synligt eller i ett skåp bredvid larmdosan då det ökar risken för lätta inbrott. Likadant gäller att koder behöver bytas regelbundet och hållas hemligt för utomstående vilket görs genom att inte trycka in koden framför någon eller placera larmdosan på ett ställe med mindre insyn. Enklare enheter sätter större krav på användarna vilket är en större utmaning enligt intervjuperson tre.

Intervjupersonerna fick svara på frågan vilka utmaningar de ser med företagets vision kopplat till säkerhet och integritet. Intervjuperson sex ansåg att utmaningen är att smarta hem kommer med säkerhetsutmaningar, det sätter höga krav på hur data hanteras och på hur systemen arbetar tillsammans med andra enheter. Genom att koppla upp fler enheter från andra tillverkare på samma system måste leverantören kunna försäkra användarnas säkerhet och integritet genom att de andra enheterna inte kan påverka säkerhetssystemet eller kan komma åt information som tillhör användarna. Intervjuperson sju såg det som en utmaning att nå ut och göra det så enkelt som möjligt för användarna samtidigt som man har kontroll över säkerheten via app och webbsida. Precis som intervjuperson åtta nämnde i tidigare fråga att med enkelheten kommer det risker. Till sist menar intervjuperson tre på att där inte fanns så många utmaningar kopplade till användarnas säkerhet och integritet då företaget är väldigt försiktig med information och vilka samarbeten de väljer att ta. De skulle helt enkelt inte introducera en produkt som skulle kunna äventyra individernas säkerhet eller integritet.

4.5 Faktorer som påverkar användandet av digitala säkerhetssystem

4.5.1 GDPR

Samtidigt som GDPR bidrar med en större säkerhet för användarna bidrar det även till en större utmaning för företagen. Till en början använder de sig av tillfälliga koder när de behöver inträde i systemen som raderas direkt när de går därifrån. Intervjuperson tre berättar: “Vi har enormt dryga system”, med detta menar denne personen att när något är drygt, då är det säkert. Mail och inloggning i system kräver att de loggar in varje gång med användarnamn och lösenord för att sedan få en kod skickad som till sist släpper in användaren i systemet. Sedan denna lag introducerades berättade intervjuperson tre att de behövt vidta några åtgärder för att inte äventyra någons integritet eller säkerhet. De började sätta upp kodlås i arkivrum, tömma bilen på papper och aldrig lämna några papper eller dokument synliga någonstans. GDPR ställer krav på företagen som ger de anställda och användarna mer arbete och det är svårare att komma åt uppgifter och system för att kunna följa lagarna samtidigt som de levererar en säker produkt. De tre intervjupersonerna instämmer om den svåra balansen att leverera den bästa säkerheten utan att göra intrång på någons integritet och säkerhet.

4.5.2. Integritet

Att kunna säkerställa användarnas integritet är en utmaning när det kommer till att leverera ett säkerhetssystem. Att bevisa att man enbart övervakar kameror vid larm är svårt och det kräver ett större förtroende mellan användare och leverantör. Intervjupersonerna från den valda leverantören menar på att de jobbar för att försäkra integriteten genom att ständigt uppdatera sig om lagar och regler och informerar tydligt hur de hanterar kundernas uppgifter och följer lagens ramar vid installation av systemet. De lägger stor vikt på det allvar som tas när det kommer till uppgifter och data som samlats, ingen information lämnar företaget och de som arbetar i fält behöver använda sig av autentisering för att komma åt uppgifter (Intervjuperson tre).

5 Analys

De intervjuer som genomförts med användare av det digitala säkerhetssystemet och representanter från leverantören ger värdefulla insikter i användarnas perspektiv på det digitala hem- och säkerhetssystemets möjligheter och utmaningar. Genom att analysera svaren ur både användar- och företagsperspektiv kan vi identifiera huvudteman och dra kopplingar mellan dem.

Förbättrad säkerhet och sinnesfrid

Både användare och leverantörens representanter betonade den ökade känslan av säkerhet och sinnesfrid som det digitala säkerhetssystemet ger. Användare lyfte fram funktioner som fjärrövervakning, omedelbara aviseringar och möjligheten att kontrollera sina hem även när de är borta. Vilket även kan kopplas och stärkas av den studie som gjordes av Marklund och Tollin där resultaten visade att respondenterna kände sig trygga och bekväma när kameraövervakning används i syftet att motverka brott. Dessutom bidrar denna tillgänglighet och realtidsinformation till en större känsla av säkerhet för användarna. Leverantörens fokus på att erbjuda snabba svarstider och aktivt engagemang med kunder förstärker denna känsla av säkerhet ytterligare. Företagets arbete inhouse och gentemot sina kunder kan kopplas till begreppet CIA där konfidentialitet, integritet och tillgänglighet är nyckelfaktorerna för informationssäkerhet, med informationssäkerhet kommer en trygghet och säkerhetskänsla hos användarna som även stärker förtroendet mellan leverantör och användare. Intervjupersonerna sex och åtta nämnde båda två vikten som företaget lägger på konfidentialitet och integritet och det förändringsarbete som företaget gjort för att försäkra sig om att kundernas data hålls säker. Konfidentialitet kan i detta arbete kopplas till GDPR-lagarna som tvingat företag att införa säkrare hantering av dokument och data för att inte skada den personliga integriteten, det samma gäller okränkbarhet där användarna behöver informeras och godkänna eventuella ändringar. Till sist finns informationen tillgänglig för användarna, dels att de ständigt har tillgång till appen och dels att företaget skickar ut mail och har ett aktivt engagemang med kunderna.

Användarvänlig app och system
Intervjupersonerna betonade vikten av en intuitiv och lättanvänd app för att hantera säkerhetssystemet. Användarna uppskattade appens navigering, möjligheten att ge åtkomst till andra användare och bekvämligheten med att kontrollera systemstatus och kameraflöden. Leverantörens betoning på att tillhandahålla en användarvänlig app stämmer överens med användarnas förväntningar och bidrar till en positiv användarupplevelse.

Framtidsmöjligheter
Användarna tillfrågades om det digitala säkerhetssystemets framtida potential. Representanter för leverantören nämnde att utöka systemets kapacitet genom att integrera ytterligare smarta enheter och tjänster. Detta överensstämmer med användarnas önskemål om fler funktioner, såsom anpassade säkerhetszoner och förbättrad design på enheterna. Betoningen på kontinuerlig förbättring och innovation tyder på att leverantören strävar efter att möta föränderliga användarbehov och preferenser.

Utmaningar och områden för förbättring
Både användare och leverantörens representanter erkände vissa utmaningar och områden för förbättring. Användare nämnde oro för falsklarm som utlösts av husdjur, kostnaden för ytterligare funktioner och potentiella integritetsproblem. De lyfte också fram behovet av bättre placering för enheterna och enklare batteribyte processer. Leverantörens representanter erkände behovet av snabbare e-postsvar, minskade telefon väntetider och mer proaktiv kommunikation med kunder. Dessa insikter ger värdefull feedback för företaget för att hantera användarproblem och förbättra deras tjänster.

Intervjuerna visar på konvergens perspektiv mellan användare och leverantörens representanter. Båda sidor inser vikten av att tillhandahålla en säker och användarvänlig upplevelse. Användare uppskattar det digitala säkerhetssystemets förmåga att förbättra sin vardag och erbjuder sinnesfrid och bekvämlighet genom fjärråtkomst och övervakning. Företagets fokus på lyhördhet, funktionalitet och ständiga förbättringar ligger i linje med användarnas förväntningar och föreslår ett kundcentrerat tillvägagångssätt. Dessutom delar användare och leverantörens representanter en vision för framtida möjligheter. Integrationen av ytterligare smarta enheter, förbättrade anpassningsalternativ och förbättrade kommunikationskanaler återspeglar deras gemensamma strävan att skapa ett heltäckande och anpassningsbart säkerhetssystem. Men även utmaningar och förbättringsområden framgår av intervjuerna. Användarnas oro angående falsklarm, kostnader, enhetsplacering och batteribyte framhäver specifika smärtpunkter som leverantören bör åtgärda. Behovet av bättre kommunikation och utbildning, som uttrycks av användare, understryker vikten av att utbilda kunder om appanvändning och systemfunktioner.

Sammanfattningsvis avslöjar intervjuerna en positiv användarupplevelse av det digitala säkerhetssystemet, driven av en kombination av förbättrad säkerhet, användarvänliga funktioner och potentialen för framtida framsteg. Leverantörens engagemang för kundnöjdhet och ständiga förbättringar är uppenbart i deras ansträngningar att ta itu med användarproblem och anpassa sig till förändrade behov. Genom att ta itu med de identifierade utmaningarna

och bygga vidare på användarnas positiva feedback kan företaget ytterligare stärka sin position som en pålitlig leverantör av digitala säkerhetssystem och smarta hem.

Ur ett etiskt perspektiv är det viktigt att överväga konsekvenserna av betydelsefull teknik för användarnas integritet, säkerhet och välbefinnande (Verbeek, 2011). Verbeeks (2011) etiska perspektiv, som är förankrat i teknikfilosofin, kan ge insikter i dessa överväganden. Verbeek betonar idén att teknologier inte är neutrala verktyg utan aktivt formar vår uppfattning, upplevelser och interaktioner med världen. När det gäller Leverantörens digitala säkerhetssystem lyfts användarnas erfarenheter och uppfattningar fram. Systemet beskrivs som att det ger en känsla av säkerhet och sinnesfrid för användarna, vilket gör att de kan övervaka sina hem på distans och ta emot varningar vid eventuella hot eller incidenter. Denna aspekt överensstämmer med Verbeeks föreställning om teknik som en medlare som påverkar vår uppfattning och våra känslor (Verbeek, 2011). Dessutom framhävs av intervjuerna den positiva effekten av det digitala säkerhetssystemet på användarnas dagliga liv, såsom möjligheten att enkelt kontrollera säkerheten i sina hem, övervaka temperaturen och kontrollera åtkomst genom funktioner som specifika tidsbegränsade koder. Dessa funktioner visar hur systemet kan förbättra användarens bekvämlighet och kontroll över sin livsmiljö. Verbeeks perspektiv uppmuntrar oss att överväga de etiska implikationerna av dessa teknologier i termer av användares autonomi och handlingsfrihet i att forma sina miljöer.

Men det finns även utmaningar och problem som användarna tar upp. Dessa inkluderar ökad medvetenhet och oro om säkerhet, såväl som frågor relaterade till husdjur som utlöser falsklarm, höga kostnader och svårigheter att få tag i specifika ersättningsbatterier. Ur ett etiskt perspektiv är det viktigt att ta itu med dessa utmaningar och se till att tekniken respekterar användarnas integritet, tillhandahåller tillförlitliga och prisvärda tjänster och beaktar inverkan på icke-mänskliga enheter (t.ex. husdjur) i hemmet (Verbeek, 2011). Verbeeks etiska perspektiv uppmuntrar oss att reflektera över de moraliska värderingar som är inbäddade i design, implementering och användning av teknologier. Den betonar vikten av att ta hänsyn till den mänskliga erfarenheten, samhälleliga konsekvenser och potentialen för maktobalansen när man använder och reglerar sådan teknik. När man utvärderar leverantörens digitala säkerhetssystem är det väsentligt att analysera systemets inverkan på användarnas välbefinnande, deras känsla av säkerhet och kontroll, samt rättvisa, transparens och ansvarsskyldighet hos företaget bakom tekniken. Däremot skriver IDG Expert Network (2018) att säljare, tillverkare och utvecklare inom IoT behöver numera lägga större fokus på produkternas säkerhet och implementera säkerhet när det kommer till integritet och personuppgifter, redan vid uppstarten. Företagen behöver tydligt informera användarna om hur de använder den data som samlas in. Skulle personen ge samtycke till att dennes information samlas in har personen rätt till att välja ut vilken information de får ta del av. Dessa regler är en möjlighet för användarna att kunna känna sig säkra och att deras integritet inte påverkas vilket i sin tur skapar ett större förtroende för företaget.

RITE-principerna agerar som ett komplement till CIA-principerna som nämndes tidigare och tillsammans bildar de den kompletta informationssäkerheten. RITE kan däremot kopplas vidare till den bild som företaget vill presentera för användarna. I detta fallet har företaget ett

stort ansvar att se till att hålla kundernas data säkert och bidra med ett säkerhetssystem som användarna kan känna sig trygga med. Integriteten är densamma som ses i CIA begreppet. Förtroendet är en stor del för att kunderna ska implementera deras system då de lägger sina hem i företagets händer. Ett exempel på detta kan dras med de skandaler som drabbade leverantörens kunder när anställda tog del av opassande bilder, vilket vidare kan kopplas vidare till de etiska frågorna. Att ha dessa principer i åtanke är därför av större vikt för att företagen ska kunna leverera korrekt informationssäkerhet till sina kunder som leder till att kunderna känner sig trygga och säkra i sina hem och att de i framtiden eventuellt kan känna sig trygga oavsett var de befinner sig tack vare Guardian.

6 Slutsats

Syftet att besvara frågan "*Hur upplever användare och leverantören användningen av digitala säkerhetssystem i smarta hem?*" har uppfyllts genom en djupgående analys utifrån det empiriska material som hämtats från de semistrukturerade intervjuerna tillsammans med teorin som presenterats.

Resultaten av denna studie visar på en intressant aspekt när det gäller användarnas förtroende för digitala säkerhetssystem, särskilt i samband med smarta hem. Trots begränsad kunskap om systemets inre funktion och begränsad hänsyn till deras integritet, visade användarna en betydande nivå av förtroende för det digitala säkerhetssystemet. Det är anmärkningsvärt att de upplevda fördelarna och möjligheterna som systemet erbjuder uppvägde de potentiella utmaningarna och problemen. Detta indikerar att Leverantören effektivt har uppnått sina mål att skapa användarnas förtroende för deras digitala säkerhetssystem.

Användarnas förtroende för systemet, även utan djup teknisk kunskap eller omfattande sekretessöverväganden, understryker betydelsen av effektiv kommunikation och design av användarupplevelser. Leverantörens förmåga att ingjuta förtroende hos sina kunder tyder på framgångsrik implementering av strategier som prioriterar bekvämlighet, sinnesfrid och användarvänlighet. Det är dock viktigt att inse de etiska konsekvenserna och potentiella integritetsproblem som är förknippade med dessa system. Eftersom användare i allt högre grad förlitar sig på digitala säkerhetssystem, blir det absolut nödvändigt att utbilda dem om de potentiella riskerna och uppmuntra dem att aktivt engagera sig i integritetsskyddande åtgärder. Framtida forskning bör gräva djupare i förståelsen av användarnas attityder till integritet, de avvägningar de är villiga att göra och effektiviteten hos olika kommunikationsstrategier för att ta itu med dessa problem.

Slutligen visar den här studien på det starka förtroende som användare uppvisar för leverantörens digitala säkerhetssystem, vilket belyser företagets framgång med att nå sina mål. Även om de möjligheter som systemet erbjuder uppvägde utmaningarna i användarnas uppfattningar, är det viktigt att vara vaksam när det gäller att ta itu med etiska överväganden och integritetsfrågor. Genom att främja transparens, användarutbildning och ansvarsfull praxis kan den digitala smarta hemindustrin fortsätta att tillhandahålla säkra och bekväma upplevelser för husägare samtidigt som de skyddar deras integritet och välbefinnande.

Sammanfattningsvis visar analysen av intervjuer med användare och leverantörens representanter ger värdefulla insikter om möjligheter och utmaningar med digitala hem- och säkerhetssystem. Användare värdesätter förbättrad säkerhet, sinnesfrid och användarvänlighet, medan leverantören betonar snabba svarstider och kundengagemang. Framtida möjligheter inkluderar integrering av smarta enheter och förbättrade anpassningsmöjligheter. Men utmaningar som falsklarm, kostnader och batteribyte processer måste åtgärdas. Trots begränsad kunskap och integritethänsyn visar användarna förtroende för systemet, vilket understryker vikten av effektiv kommunikation och design av användarupplevelser. Etiska perspektiv och medvetenhet om integritet implikationer är avgörande. Det är nödvändigt att utbilda användare och uppmuntra deras aktiva engagemang i integritetsskyddande åtgärder. Framtida forskning bör utforska användarnas attityder till integritet och utvärdera kommunikationsstrategier.

6.1 Vidare forskning

Med studien i beaktande finns det en del intressanta perspektiv att forska djupare inom. Med tanke på studiens omfattning har flera frågor behövts skalas bort och många perspektiv fått avgränsas. Till en början hade vidare forskning kunnat leda till att kolla djupare inom flera leverantörer för att få en större helhetsbild samt för att öka trovärdigheten ännu mer, då de flesta som använder sig av leverantörens hemlarm verkade extremt nöjda. Vidare hade det kunnat forskas djupare i hur dessa effekter påverkar både användare och företag samt addera fler perspektiv som exempelvis ännu mer etik. Med tanke på de framtidsvisioner som företaget idag besitter hade mer tid kunnat läggas på att se hur framtidens teknologi skapar möjligheter och utmaningar för både företag och användare. Vi kan även se en annan möjlighet som är relevant i dagens samhälle är hur dessa smarta enheter kan bidra till en bättre miljö med hjälp av att koppla in nya enheter och styra hemmet mer ekonomiskt och miljövänligt.

Referenslista

Alaba, F. A., Adetunmbi, A. O., & Daramola, O. (2017). Internet of Things (IoT) security: A survey. Journal of Network and Computer Applications, 88, 10-28.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

Aschberg, R., Mohlin, L. (2022). *200 sekunder - Falsk trygghet del 1 & 2* [Program] Aftonbladet. https://tv.aftonbladet.se/kategori/99/200-sekunder

Balakrishnan, S. Vasudavan, H. Murugesan, R, K. (2018). *Smart Home Technologies: A Preliminary Review.* Association for Computing Machinery. New York, USA

Brown, I., & Adams, A. A. (2007). The ethical challenges of ubiquitous healthcare. *The International Review of Information Ethics*, *8*, 53–60.

Bugeja, J., Jacobsson, A. and Davidsson, P. (2016) On Privacy and Security Challenges in Smart Connected Homes. 2016 European Intelligence and Security Informatics Conference, Uppsala, 17-19 August 2016, 172-175.

Carlsson, B. Jacobsson, A. (2012). *Om säkerhet i digitala ekosystem*. Studentlitteratur, Lund.

Denscombe, M. (2018). *Forskningshandboken.* Studentlitteratur, Lund

Digitaliseringskommissionen (2016). Digitaliseringens effekter på individ och samhälle - fyra temarapporter. (SOU 2016:85). Stockholm.

Englund, A. (2018). *GDPR och internet of things – fem saker du behöver känna till.* IDG Expert Network. https://computersweden.idg.se/2.2683/1.697169/gdpr-och-iot?fbclid=IwAR1coVUw8NIkuxzbQvOXYSbAtHzLGt5kBFb48ZbW14DhG7Xnz9bBoPbkiN4

Forskning. (2016). *Digitalisering förändrar hela vår värld. https://www.forskning.se/2016/04/12/digitaliseringen-forandrar-hela-var-varld/#*

Gravina, R., Palau, C. E., Manso, M., Liotta, A., & Fortino, G. (2017). *Integration, Interconnection, and Interoperability of IoT Systems. Springer International Publishing AG.*

Gray, J. & Rumpe, B. (2017). Models for digitalization. Software & Systems Modeling. Volume 16, Issue 59, Pages 1-2.

Hallberg, P. (1978). *Hermeneutik.* Samlaren - tidskrift för svensk litteraturvetenskaplig forskning. Uppsala: Svenska Litteratursällskapet

Internet of Things Sverige. (u.å.). *IoT - så funkar det. https://iotsverige.se/iot-sa-funkar-det*

Kajtazi, M. (2013). *Assessing Escalation of Commitment as an Antecedent of Noncompliance with Information Security Policy*. Linnaeus University Press, Växjö

Mansfield-Devine, S. (2016) *Securing the Internet of Things - Computer Fraud & Security*, Volume 2016, Issue 4, Pages 15-20 https://www.sciencedirect.com/science/article/abs/pii/S1361372316300380

Marklund, F. & Tollin, K. (2020). *Kroppsburna kameror: en utvärdering av pilotverksamhet i polisregion Stockholm. Stockholm: Brottsförebyggande rådet*. https://www.bra.se/download/18.cba82f7130f475a2f1800015488/1371914730522/2003_kameraovervakning_i_brottsforebyggande_syfte.pdf

Microsoft Azure. (u.å.). What is Cloud computing? https://azure.microsoft.com/en-in/resources/cloud-computing-dictionary/what-is-cloud-computing

Miller, M. (2015). *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World. Indianapolis: Que*

Norrgrann, K. Mohlin, L. Aschberg, R. (2022). *”Ingen ska behöva bli filmad så i sitt eget hem”*. Aftonbladet. https://www.aftonbladet.se/nyheter/a/rEJX38/tidigare-anstallda-pa-verisure-berattar-bilder-av-nakna-kunder-cirkulerade-internt-200-sekunder-granskar

Oates, B.J. (2006). *Researching information systems and computing.* London: SAGE.

Oates, B. J., Griffiths, M., & McLean, R. (2022). Researching Information Systems and Computing (2:a uppl.). SAGE Publications Ltd.

Petersson, E., Sördal, T. (2018) *Det Smarta Hemmet - Användarnas förtroende för de smarta enheterna i hemmet.* Institutionen för Informatik, Lunds Universitet. *https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8946051&fileOId=8946066*

Saizmaa, T., Kim, H-C. (2008). *Smart Home Design: Home or House? Convergence and Hybrid Information Technology - Volume 01. https://ieeexplore.ieee.org/document/4682016*

Sfar, A. Natalizio, E. Challal, Y. Chtourou, Z. (2017) *A roadmap for security challenges in the Internet of Things*. Digital Communications and Networks. Volume 4, Issue 2, April 2018, Pages 118-137.

Teknikföretagen. (2021). *Svensk utveckling under 125 år. https://www.teknikforetagen.se/vi-skapar-losningarna/artiklar/svensk-teknikutveckling-under-125-ar/*

Thurén, T. 2007. Vetenskapsteori för nybörjare. 2:a upplagan. Liber, Malmö.

Verbeek, P. (2011). *Moralizing technology: understanding and designing the morality of things*. Chicago: University of Chicago Press

Verbeek, P. Tijink, D. (2020). *Guidance ethics approach: An ethical dialogue about technology with perspective on actions*. Platform voor de InformatieSamenleving

Östlund, B. (Programledare). (2021). *Hackad [TV-program]. Svt. https://www.svtplay.se/hackad*

Bilagor

Bilaga 1 - Intervjufrågor till användare

Introduktionsfrågor

1. Hur många bor i hushållet?
2. I vilket åldersspann är ni som bor i hushållet?
3. Hur stor kännedom har ni kring smarta hem?
4. Hur ser ni på säkerhet i hemmet? Gör det att ni känner er tryggare?
5. Hur upplever ni att er integritet påverkats sedan ni installerade ert säkerhetssystem?

Frågor om leverantören

6. Varför valde ni denna leverantör?
7. Hur länge har ni använt er av deras system?
8. Har ni haft något annat system tidigare? Om ja, finns det någon tydlig skillnad?
9. Vilka enheter använder ni er av?
10. Är det något som gör er extra nöjda med systemet?
11. Är det något som ni är missnöjda med eller som ni tycker kan förbättras?

Fördjupningsfrågor

12. Vilka möjligheter bidrar deras app med i er vardag?
13. Upplever ni att appen bildar utmaningar i er vardag?
14. Upplever ni att er vardag förändrats sedan ni installerade systemet och i så fall hur?
15. Hur jobbar ni för att använda det digitala säkerhetssystemet så säkert som möjligt?
16. Om det är något ni kan förändra med leverantören, vad skulle det vara?

Allmänna frågor

17. Hur har ni fått kännedom av appen? Utbildning osv.
18. Upplever ni att servicen är snabb på andra hållet om något skulle strula med enheterna?
19. Hur upplever du att tjänsten hjälper dig om du skulle göra ett misstag?
20. Finns det några vanliga problem som brukar uppstå när du använder tekniken?

Bilaga 2 - Intervjufrågor till leverantörens representanter

Introduktion

1. Hur länge har du jobbat i företaget?
2. Hur kommer det sig att du började jobba på detta företag?
3. Har du avancerat inom företaget eller var detta den första positionen du fick?

Om Företaget

4. Hur skiljer sig företaget från era konkurrenter?
5. Hur arbetar ni på företaget för att förbättra säkerheten?
6. Hur arbetar ni för att försäkra användarnas integritet?
7. Vilka möjligheter ser ni att ert system kan bidra med till användarna?
8. Vilka utmaningar finner ni i det digitala säkerhetssystemet?
9. Vad händer om appen eventuellt skulle krascha?
10. Vad händer om appen eventuellt skulle hackas?
11. Vilka utmaningar ser ni med er vision kopplat till säkerhet och integritet?

Framtiden

12. Vilka möjligheter tror ni att systemet kan bidra med inom en 5/10 års period?
13. Vilken påverkan har företaget på säkerheten i framtiden?
14. Hur ser ni på företagets framtid, vad har ni för “mål”?