Teknik och samhälle
Datavetenskap

Examensarbete
15 högskolepoäng, grundnivå

Datahantering i smarta hem:
En studie om hur data från smarta hem hanteras av företag

Datamanagement in smart homes:
A study of how data from smart homes is managed by companies

Martinsson Karolin
Shirazi Angelica

Examen: Kandidatexamen 180 hp
Huvudområde: Datavetenskap
Program: Informationsarkitekt
Datum för slutseminarium: 2012-05-29

Handledare: Helena Holmström Olsson
Examinator: Carl Johan Orre

Sammanfattning

Smarta hem är ett koncept som har utvecklats i hög takt under de senaste åren. Enheter som kylskåp, lampor och dörrar i bostäder kopplas upp och kan sedan styras med hjälp av en mobil för att underlätta i vardagen. Eftersom dessa uppkopplade enheter samlar in data om oss blir säkerhet och integritet något som diskuteras flitigt. I denna uppsats presenteras resultatet från intervjuer som har gjorts med fyra olika företag som säljer produkter som samlar in data från internet of things-enheter. Tre av dessa företag säljer internet of things-enheter till smarta hem. Syftet är att se hur dessa företag hanterar datainsamling från sina kunder och vilka utmaningar de ställs inför i det arbetet samt om detta påverkar kundernas integritet och säkerhet.

Nyckelord: Smarta hem, Internet of Things, Säkerhet, Integritet, Molnlösning

Abstract

Smart homes is a concept that has been developed rapidly the last years. People connect devices like refrigerators, lightning and doors in their homes that they can control with their smartphones to facilitate in their everyday life. Since these connected devices collect data about us, security and privacy is something that is discussed frequently. In this thesis we present the result from interviews that is conducted with four different companies that sell products that gather data from internet of things units. Three of these companies sell IoT products for smart homes. The purpose is to show how these companies handle collected data from customers and what challenges they face in this work and if that affects the customers.

Keywords: Smart homes, Internet of Things, Security, Integrity, Cloud Storage

Innehåll

1 Inledning

De senaste åren har antalet Internet of Things-enheter, ofta förkortat IoT-enheter, i världen ökat och den trenden väntas fortsätta [6]. Precis som namnet avslöjar är enheterna uppkopplade till internet och benämns därför som "smarta". IoT-enheter innefattar mobiler, klockor, larm, markiser, skor, eluttag och bilar för att nämna några få exempel. Dessa enheter används exempelvis för privat bruk, i våra hem, inom äldrevården, för infrastrukturen i våra städer och för att minska förbrukningen av energi [18]. Möjligheterna med IoT-enheter är stora eftersom dess applikationer samlar in massor av data. De kan därför ge bättre förståelse för hur vi människor lever, hur våra städer fungerar och mycket mer [18]. Data kan även användas för stadsplanering och ge kontroll för att kunna minska förbrukningen av energi och avfall. Även inom äldrevården kan IoT-enheter vara fördelaktiga där de kan påminna en person som har alzheimers att stänga av spisen när hen har lagat mat eller påminna hen att ta sin medicin vid en viss tidpunkt.

Även våra hem blir allt mer utrustade med IoT-enheter. Smarta hem är en benämning på hem som är utrustade med IoT-enheter som är anpassade för hemmet, såsom smarta kylskåp. Smarta hem ämnar till att underlätta vårt vardagsliv och tillför många fördelar. Ett smart kylskåp filmar insidan av kylskåpet som sedan kan användas som ett hjälpmedel i affären, om det finns en osäkerhet kring vad som behövs handlas hem. Det kan också vara smarta eluttag, smart tv, smart hemlarm som bevakar hemmet när ingen är hemma, smarta vattendetektorer som känner av vattenläckor och mycket mer. Temperaturen kan exempelvis ställas in beroende på om någon är hemma eller inte. Det kan även säkra hem från inbrott och bränder [27]. För att kunna bidra med dessa bekvämligheter, innebär det också att dessa smarta enheter samlar in data kring våra vanor och vårt vardagliga liv, vilket kan uppfattas som ett hot mot den personliga integriteten. Ett exempel på detta kan vara data som samlas in från brandlarm som har en inbyggd kamera. Vid rök sätts kameran igång och automatiskt så kontaktas larmcentralen för att de ska kunna kontrollera om det finns rök. Det kan diskuteras om hur man är säker på att kameran endast är igång när det finns rök. Om kameran skulle sättas igång utan någon rök i hemmet, kan detta upplevas som ett integritetsbrott mot privatpersonen för att den endast har gått med på att bli filmad vid rök [9].

Samtidigt som fördelarna med uppkopplade enheter i våra hem är många, så finns det även risker med detta. Det kan finnas stora säkerhetsrisker med system som är uppkopplade mot internet, eftersom det gör dem extra utsatta för attacker. Detta är för att de är dynamiska, har hög rörlighet och är heterogena vilket gör att de kan kommunicera och skicka protokoll till andra IoT-enheter [6]. Eftersom dessa IoT-enheter är sårbara och samlar in vad som kan uppfattas som personlig data, syftar denna uppsats till att se hur företag hanterar denna data som samlas in från IoT-enheter i hemmet. Vi vill utmärka vilka utmaningar som upplevs av företag när de samlar in data från deras kunder i smarta hem och om detta påverkar kundernas säkerhet och integritet. Vi vill även upplysa om vilket ansvar företagen som vi har intervjuat anser sig ha över kundernas integritet och säkerhet vid datainsamling.

1.1 Syfte

Denna uppsats ämnar undersöka hur företag idag hanterar data som samlas in från deras kunder via IoT-enheter i smarta hem. Studien ger en förståelse för hur kundernas privata data lagras och används av företag. Vi undersöker vilka utmaningar företag ställs inför i arbetet med datainsamling och vilken påverkan detta har på kundernas säkerhet och integritet. Slutligen tar vi reda på vilket ansvar företag anser sig ha för kundernas integritet och säkerhet vid datainsamling från IoT-enheter i smarta hem.

1.2 Frågeställning

Q1 *Vilka utmaningar ställs företag inför när de samlar in data från sina kunder och påverkar detta kundernas integritet eller säkerhet?*

Q2 *Hur hanterar och lagrar företag och leverantörer insamlad data från sina kunder?*

Q3 *Vilket ansvar upplever företag att de har gentemot sina kunders integritet och säkerhet vid datainsamling från IoT-enheter i smarta hem?*

1.3 Avgränsning

Denna uppsats ska främst fokusera på företags arbete kring datainsamling i smarta hem och vilka utmaningar de ställs inför i det arbetet. Alla fyra företag som vi har intervjuat säljer IoT-enheter och således arbetar de alla med att samla in data från kunder. Tre av företagen erbjuder produkter som används i smarta hem såsom övervakningskameror, energistyrning och sensorer. Det fjärde företaget valde vi att ha med trots att de inte säljer typiska smarta hem-produkter, eftersom de arbetar med insamlad data från privatpersoner. Detta företag benämns som Företag 2 i vår uppsats.

Företagen som har intervjuats är alla belägna i Malmö. Tre av företagen finns dessutom i andra länder än Sverige och alla har kunder lokaliserade i olika delar av Europa.

Uppsatsen går inte djupt in på det tekniska, såsom hur protokoll fungerar eller hur produkter pratar med varandra. Istället presenteras hur och vilken data som samlas in från kunder samt hur denna hanteras utav företagen i förhållande till säkerhet och integritet. Lagar som påverkar hur detta hanteras förklaras även för att ge läsaren en bredare förståelse.

1.4 Målgrupp

Målgruppen för detta arbete är kunder som har köpt IoT-enheter för smarta hem samt utvecklare och leverantörer av smarta hem-produkter.

2 Definition av begrepp

I denna del definieras begrepp som används i uppsatsen. Begreppen förklaras för att ge en förståelse för begreppen samt hur dessa hänger samman.

2.1 Internet of Things

IoT, eller Sakernas internet på svenska, är ett samlingsbegrepp för den utveckling som innebär att maskiner, fordon och andra saker blir uppkopplade till internet med hjälp av inbyggda sensorer eller processorer [26]. IoT möjliggör fysiska objekt att höra, se, tänka och utföra handlingar [1]. Tack vare det kan de uppfatta sin omvärld och kommunicera med andra enheter utan att vi människor behöver vara involverade. Enheter som är uppkopplade kan vara allt från mobil, surfplattor, smartklockor och kylskåp. Ett exempel på hur IoT kan underlätta vardagen är att elementet hemma stänger av sig mellan 8.00-17.00 varje dag, eftersom ingen är hemma vid den tidpunkten. Ett annat exempel är att det visas på din klocka när någon ringer till din mobil och du kan också svara genom klockan.

IoT-enheter som kopplas upp i hemmet är något som blir allt mer vanligt. Lampor, kameror och kylskåp kopplas upp i hemmet, för att sedan kunna kontrolleras via privatpersonens mobil. Privatpersonen kan exempelvis se att hens barn har kommit hem säkert eller låsa ytterdörren via mobilen när detta har glömts bort. Det kan även göras stora energibesparingar tack vare IoT [5]. Enheterna kan sänka värmen automatiskt när ingen är hemma och ställa tvn på standby-läge när ingen längre tittar på tv. Detta gynnar både miljön och minskar din energikostnad.

IoT har gjort att fysiska objekt har gått från traditionella till smarta tack vare underliggande tekniker så som ubiquitous and pervasive computing, inbäddade enheter, kommunikationstekniker, sensornätverk, internet-protokoll och applikationer [1]. Utvecklingen av IoT går väldigt snabbt och antalet IoT-enheter ökar för varje dag som går.

I framtiden tror man att IoT kommer ha stor betydelse i både hem- och affärssammanhang för att underlätta i vardagen och förbättra ekonomin i världen. Eftersom IoT kan användas och underlätta i många olika sammanhang räknar man med att 50 miljarder enheter kommer vara uppkopplade år 2020 [5]. För att kunna realisera detta krävs det att teknologier, applikationer och innovationer växer proportionellt med marknadens behov [1].

2.2 Molnlagring

Molnlagring, på engelska cloud storage, innebär att användare kan skicka sin data och lagring till databaser på internet, så kallade moln [35].

Molnlagring underlättar för användaren på så sätt att man slipper upprätthålla resurser på egen hand. Man har tillgång till sina dokument när som helst och från var som helst. Man kan sitta vid vilken dator och vara uppkopplad till vilket nätverk som helst och ändå ha tillgång till sina filer. Det ger även möjligheten för flera personer att arbeta på samma dokument samtidigt och se ändringar direkt när de görs, exempelvis med tjänsten Google Docs [3]. Molnlagring används i många olika syften, till exempel för att dela en Powerpoint på jobbet, lagra bilder i privat bruk eller dela dokument som andra människor ska kunna se. Exempel på molntjänster är Open Office, Dropbox och Flickr [38]. Risken med molnlagring är att data finns på en annan server och det är någon annan som upprätthåller din data. Därför är många oroliga över säkerheten och integriteten i molntjänster [35].

IoT-enheter producerar mycket stora mängder data men har en begränsad kapacitet till att lagra och bearbeta den data som de samlar in [5]. Därför förlitar sig dessa enheter ofta på de stora möjligheter som finns med molnlagring. Molnlagring har enorma möjligheter till att hantera och och analysera data och har därför stor betydelse för IoT-system. Olika

företag som säljer IoT-enheter till smarta hem lagrar sin data på olika sätt. En del har databaser som företaget själv har skapat och som bara de har tillgång till. Andra skickar sin data till molnet, som då kontrolleras av andra parter.

2.3 Smarta hem

Ett smart hem kan definieras som en bostad som innehåller sensorer, system och IoT-enheter som kan fjärrstyras, kontrolleras och övervakas med hjälp av ett kommunikationsnätverk [8]. Kumar et al. [27] beskriver i en artikel smarta hem som en teknisk utveckling som används för att övervaka och styra hemmet genom samordnade nätverk och tekniker. I ett smart hem använder man sig av IoT-enheter som samlar in data om de som bor i hemmet genom sensorer, kameror, mikrofoner och andra enheter. Dessa enheter samlar in information om våra vanor i hemmet, exempelvis när vi brukar låsa dörren varje dag och hur varmt vi har det i huset. Med hjälp av denna data kan hemmet sedan anpassas efter de boende och dess vanor. De senaste åren har intresset för design och implementation av smarta hem ökat rejält [29]. Det finns en stor efterfrågan på IoT-enheter som är anpassade till smarta hem och många konsumenter har fått intresse och blivit medvetna om vad det innebär [31].

Ett ord som ibland nämns som synonym till smart hem är hem-automatisering. Det innebär att hemmet är automatiserat och att IoT-enheter med hjälp av nätverk och tekniker kan göra saker som underlättar för den boende [31]. Vi kan ställa in enheterna så att de gör en viss sak vid en viss tidpunkt. Till exempel kan man med hjälp av tekniken se till att kaffemaskinen sätts igång klockan 06.30 varje morgon.

Kumar et al. [27] förklarar vidare hur ett smart hem fungerar tekniskt. Som tidigare nämnt består det interna nätverket av ett antal olika enheter. De vanligaste teknikerna för automatisering i hemmet idag är Z-wave och Zigbee, som båda är anpassade för trådlös M2M (Machine to Machine)-kommunikation [21]. Andra tekniker som används för automatisering i smarta hem är X10, UPB och INSTEON.

Figur 2.3 Illustration som visar hur IoT-enheterna samverkar i smarta hem

1. IoT-enheter i ditt smarta hem som samlar in data från användaren
2. IoT-enheter som styr smarta hem-enheterna och presenterar information som samlas in för användaren.
3. Molnet som lagrar data som samlas in från användaren
4. Router som bidrar med internet i ditt hem

Alla enheter på bilden är IoT-enheter, däremot har de olika uppgifter. De enheter som finns vid huset är de IoT-enheterna som finns i ett smarta hem såsom smart kylskåp, ditt playstation, smart plugs och kaffekokaren som kokar ditt kaffe på morgonen. Med hjälp av IoT-enheterna som mobilen, surfplattan och datorn kan IoT-enheterna i hemmet styras, för att senare få statistik på eller information kring vad som har hänt. All data lagras och kan hämtas via molnet. För att allt detta ska vara möjligt krävs det internet som exempelvis kan hämtas hemifrån via en router.

3 Bakgrund och tidigare forskning

Nedan presenteras tidigare forskning som gjorts kring säkerhet och integritet i smarta hem.

3.1 Smarta hem i olika syften

Smarta hem används på flera olika områden i olika syften. Det ger oss människor enorma möjligheter på olika sätt [39]. Man kan dela in smarta hem i fyra kategorier [2], vilka beskrivs nedan.

3.1.1 Vård i hemmet/äldreomsorg

Detta område avser hjälpa människor med sysslor i hemmet [2], främst äldre människor men även andra som är i behov av hjälp. Idag lever befolkningen i genomsnitt längre och människor bor hemma längre vilket kan leda till att de behöver assistans i hemmet. Med ett smart hem kan personer vara assisterade 24 timmar om dygnet i sitt eget hem. Det är ett väldigt kostnadseffektivt sätt att förbättra vård i hemmet för människor. Många länder lägger väldigt mycket pengar på sjukvård idag och smarta hem kan vara med och minska de kostnaderna [11]. Det kan hjälpa personer att lösa problem som är relaterade till hälsa, kognitiv begränsning och handikapp [2]. IoT-enheter i ett smart hem kan exempelvis övervaka en person och kontrollera så att den utför aktiviteter vilket tyder på att den är säker. Andra produkter såsom sensorer kan samla in data om personen och utifrån det räkna ut personens fysiska och mentala status [11] Det kan även innefatta enkla saker som att påminna en person om att släcka lampan på kvällen eller att låsa ytterdörren när man går och lägger sig [34].

3.1.2 Energieffektivisering

Smarta hem kan hjälpa människor att minska sin energiförbrukning i hemmet. Hur mycket energi som går åt i ett hem beror mycket på de boendes vanor och beteenden i vardagen. De flesta använder mer energi än de behöver vilket innebär att det finns möjligheter att minska sin konsumtion [2]. Med ett smart hem kan privatpersonen släcka lampor var den än befinner sid och sänka värmen i huset när ingen inte är hemma med hjälp av ett klick i mobilen [28]. Sensorer kan känna av om tv:n inte används och stängs då av för att spara energi. Detta är inte bara bra för personerna i det smarta hemmet, utan det gör samtidigt miljön en stor tjänst [2].

3.1.3 Bekvämlighet och underhållning

Denna kategori innefattar funktionaliteter i ett smart hem som höjer bekvämligheten och underhållningen för de boende i hemmet. Det finns till exempel smarta lampor som ändrar färg i rummet och högtalare i olika rum som trådlöst spelar den musik man väljer i mobilen. Man kan även automatisera vissa rutiner vilket leder till höjd bekvämlighet hos de som bor i hemmet [2]. Idag finns det även system som avlyssnar det som sägs i huset och på så sätt kan man styra prylar genom sin röst. Privatpersonen kan exempelvis be systemet att släcka lampan eller låsa dörren utan att själv behöva anstränga sig [12].

3.1.4 Säkerhet

Säkerhet kan förekomma även i de andra kategorierna, till exempel kan äldre få hjälp med säkerheten i sitt hem [2]. Denna kategori avser att på olika sätt höja säkerheten i hemmet. Idag finns det flera lösningar för att hålla hemmet skyddat från obehöriga, bland annat med hjälp av larm som går direkt till ett övervakningsföretag om obehöriga kommer in i huset. Man kan även, som nämnt tidigare, låsa huset med mobilen om man skulle glömma det. Med hjälp av kameror kan man se in i huset från mobilen när man inte är hemma för att se så att det inte finns någon obehörig i huset [17]. Det finns många fler lösningar och de alla har gemensamt att de ökar säkerheten för personer i sitt eget hem. Det ger en

ökad kontroll, då privatpersonen kan ha översikt över sina barn, och kan känna sig säker på natten och kontrollera de uppkopplade produkternas status via mobilen vilket är väldigt positivt för användaren.

3.2 Dilemmat med säkerhet

Det finns ett dilemma i datasäkerhet som brukar benämnas som *"The fundamental dilemma of security"* [23]. Dieter Gollman beskriver det som följande: *"Security unaware users have special security requirements but usually no security expertise"*. Det innebär att användare och kunder till digitala lösningar ofta har krav på att säkerheten ska vara bra, men det är inte det de undersöker i första hand när de köper en produkt. De vet inte vad de kräver för säkerhetsåtgärder.

En person som inte har kompetens inom datasäkerhet kan inte göra kvalificerade beslut om säkerheten i olika produkter och kommer då få ta de produkter som anses vara standard-lösningar. Dessa standard-lösningar kanske därför inte lever upp till en kunds speciella krav, vilka hon eller han inte heller kan specificera. Som utvecklare av IoT-enheter till smarta hem blir detta en viktig sak att tänka på. Säkerheten är ett krav, men kunderna vet inte själva vad de vill eller behöver ha för säkerhet. Man måste även ta hänsyn till att ett system ska attrahera köpare och ha de senaste och bästa funktionerna.

3.2.1 Säkerhetsrisker i ett smart hem

Som tidigare nämnt finns det stora möjligheter med ett smart hem. Dock finns det även en baksida med smarta hem. Enligt Siboni et al. [36] finns det stora risker med att lämna ut information om sig och sitt hem i stor utsträckning. Mycket av den data som samlas in i smarta hem är känslig och uppfattas av användaren som privat. Data kan innehålla information om användarens vanor, hälsa och beteende.

Desto fler enheter som är uppkopplade mot ditt internet, desto mer sårbara blir enheterna för virusattacker. I tidningen Dagens Industri berättar säkerhetskonsulten Joachim Strömbergson om vad som orsakar sårbarheten. Trots att molntjänster är smidiga så blir vi också mer exponerade än vad vi är medvetna om. Detta för att data skickas till olika typer av molntjänster. Han menar att skadlig kod är fullt lika möjligt att få via smarta kylskåp som i datorn och att riskerna för intrång är lika stora. Det är dessutom inte lika självklart att det sker uppdateringar på programvaran som det är med mer kända webbläsare, vilket också utgör ett hot. Möjligheten finns att användaren inte ens är medveten om att en virusattack har skett då dessa attacker är automatiserade. Trojanska hästar är ett exempel på ett virus som installeras i dina enheter och i bakgrunden samlar in information kring dina inloggningsuppgifter från ditt nätverk [42].

David Jacoby som arbetar som säkerhetsexpert på Kapersky, provade att hacka sig in på sin egen nätverkshårddisk som hans hems IoT-enheter är uppkopplade mot och lyckades göra detta på 20 minuter. Sedan installerade han ett virus som gjorde att vem som helst kunde tillgå hans nätverk och se inloggningsuppgifter och kreditkortsinformation samt avlyssna all information. I intervjun förklarar han att folk inte är lika duktiga på att skydda hemmet som sina datorer och anser att detta bör prioriteras mer. Han lyckades hacka sig in på en router, en blu-ray spelare, en smart tv och ett bredbandsmodem [30].

I en annan artikel skriver Dagens nyheter om ett experiment som har gjorts med en webbkamera som sattes upp i en av deras reporters vardagsrum. Webbkameror används

exempelvis för övervakning av hemmet när du inte är hemma och som babymonitor. Istället för att filma hela tiden, väljer de att visa en treminutersfilm för att skydda reportens integritet. Dess nätverkskommunikation från och till webbkameran loggas hela tiden. Tre dagar efter kameran först sattes upp, upptäcktes en hackare från Italien som via ip-adressen hade lyckats se filmen. I två minuter smygtittade denna person. Kameran, som var uppe under cirka sju månader, visar att dryga 6000 personers smygtittande har registrerats och att ungefärliga fem procent av denna trafik har tillkommit från svenska ip-adresser [43].

3.2.2 Integritet och privacy

På svenska betyder integritet ett orubbat tillstånd, okränkbarhet eller oberoende [40]. Begreppet är knutet till en persons egenvärde [37]. Det finns både fysisk och psykisk integritet. Fysisk integritet innebär att ingen har rätt att undersöka en annan människas kropp utan samtycke. Psykisk integritet avser en persons värderingar, åsikter och mentala liv. En person får inte bli föremål för intrång och man får inte kränkas på grund av sina värderingar eller åsikter. Personlig integritet är rätten att inte bli kränkt. Den personliga integriteten kan hotas på flera vis, till exempel kan någon bryta tystnadsplikten och lämna ut känsliga uppgifter eller kan någon hacka din dator och hämta privat data. Personlig integritet handlar om att själv förfoga över information och att ha rätten att behålla information för sig själv.

Ett ord som används i engelskan är privacy. Det ordet går inte att direkt översätta till svenska. Många översätter det till integritet men faktum är att det inte är en helt korrekt översättning av ordet. Dictionairy.com definierar privacy som “the state of being free from unwanted or undue intrusion or disturbance in one’s private life or affairs; freedom to be let alone”. På svenska blir det alltså “tillståndet att vara fri från oönskade eller obehöriga intrång eller störningar i ens privatliv eller affärer; friheten att vara ensam” [19].

3.3 Integritet: regelverk och lagar

3.3.1 Personuppgiftslagen

Sedan 1998 har PUL, som är en förkortning för Personuppgiftslagen, funnits för att skydda personers personliga integritet från kränkning vid hantering av personuppgifter. Denna lag innefattar regler för hur bland annat registrering, insamling, lagring, spridning, utplåning och bearbetning av data får gå till. Lagen grundar sig på att personer som registeras ger sitt samtycke och får information om det [15].

Personuppgifterna kan antingen vara strukturerade eller ostrukturerade. Ett exempel på strukturerade är om de exempelvis lagras i en databas. Är uppgifterna däremot i löpande text eller i e-post anses de vara ostrukturerade. Fler regler finns för behandling av strukturerade personuppgifter än för ostrukturerade. Det finns även regler kring rättelse av felaktiga uppgifter och säkerhet. Personuppgiftsombud kan även utses av myndigheter, föreningar och företag för att försäkra sig om att personuppgifter hanteras på ett korrekt sätt [15].

Det finns annan lagstiftning där undantag fäller för PUL. Hur personuppgifter bör behandlas utav hälso- och sjukvården, socialtjänsten, skatteförvaltningen och polisen påverkas utav särregler i annan lagstiftning [15].

3.3.2 Dataskyddsreformen

Den 25 maj 2018 tillämpas ett nytt regelverk för hantering av personuppgifter som kommer att gälla i EUs alla medlemsländer. Detta innebär en del nya regler för hur personuppgifter får hanteras [14]. Mycket liknar PUL-lagen som vi har i Sverige idag men det finns några förändringar. Flera av förändringarna kommer att påverka företag som säljer IoT-enheter till smarta hem. I den nya lagen måste företag som behandlar känslig data, såsom data om hälsa eller beteende, utse en person som har till särkild uppgift att bevaka dataskyddsfrågor, ett dataskyddsombud. Den nya lagen har även en nyhet som kallas Dataportabilitet. När personuppgifter behandlas med stöd av samtycke eller avtal har den registrerade rätt att ta tillbaka de uppgifter som man själv har lämnat, för att föra över dem till en annan tjänst. Missbruksregeln som ingår i dagens lag, PUL-lagen, kommer att tas bort. Den innebär att man får behandla uppgifter i vissa situationer så länge det inte är kränkande för någon. Denna kommer alltså försvinna och sådan behandling kommer från och med den 25 maj 2018 följa förordningens regler [16].

Det har även i januari 2017, lagts fram förslag om integritet och elektronisk kommunikation som kommer att gälla internet och teleoperatörer utav EU-kommissionen. Det ersätter det nuvarande direktivet som Sverige har tillämpat i post- och telelagen [14].

3.4 Relaterade studier

Bertino et al. [7] har gjort en studie där de påpekar att det finns många säkerhetsrisker med IoT-enheter i smarta hem. Några orsaker till riskerna är att enheterna är väldigt dynamiska, föränderliga och att de inte alltid är skyddade från början. I sin studie skriver han om möjliga lösningar på säkerhetsproblemen vilka han delar upp i två kategorier; Crypthographic Solutions och Vulnerability and Intrusion Identification. Han påpekar dock att även om det finns sätt att förbättra säkerheten på, är det viktigt att komma ihåg att vi inte kan uppnå perfekt säkerhet i smarta hem [7].

Golle et al. [22] skriver i en artikel att människor är försiktiga med att lämna ut data till opålitliga parter. Hur man bibehåller personernas integritet är avgörande för hur mycket man litar på den som samlar in information. I artikeln beskrivs olika lösningar som finns för att skydda människors integritet vid datainsamling. En lösning är att anonymisera data innan det lagras, så att individuella identiteter och känslig data inte kan kopplas ihop. Anonymisering är dock inte möjligt att göra i alla sammanhang. I artikeln skriver Golle et al. [22] att det spelar stor roll hur man hanterar data för trovärdigheten. Privatpersoner är mer belägna att lämna ut känslig data om de som samlar in det har hög säkerhet och bevarar integriteten hos privatpersonen [22].

I en artikel skriver Alan Grau [24] om vem som bär ansvaret för säkerheten i ett smart hem. Han menar att företaget som erbjuder produkten främst står för säkerheten. Dock bär alla som har varit med i utvecklingen och användningen av produkten ett visst ansvar. Grau skriver vidare att företaget är ansvariga för att specificera säkerhetskrav, implementera säkerhet i enheterna och testa produkter för att säkerställa att säkerhetskraven möts. Även användaren kan själv göra flera saker för att sina enheter ska bli mer säkra. Man kan till exempel byta lösenord ofta, uppdatera enheterna och möjliggöra autentisering. Det finns fler som är med och påverkar säkerheten, bland annat företagets leverantörer och användarens bredbandsleverantör. Alla intressenter bör samverka för att säkerheten ska bli så hög som möjligt, ingen kan på egen hand få ett hem helt säkert från intrång [24].

4 Metod

Metod-avsnittet beskriver noga vilka metoder som har använts för denna uppsats. Det motiveras varför just dessa metoder användes för att svara på våra frågeställningar. Även vårt tillvägagångssätt i dessa metoder analyseras och diskuteras.

4.1 Metodbeskrivning

4.1.1 Kvalitativa metoder

Kvalitativa metoder syftar till att ge beskrivande data så som människors berättelse, känslor och reaktioner eller beteende som observeras. De olika kvalitativa metoderna som finns är bland annat observation, intervjuer och fokusgrupper[10]. Kvalitativa metoders styrka är att de ger en helhetsbild som kan ge en ökad förståelse kring en situation och olika sammanhang [25]. Vi har i vår studie valt att göra en form av intervjuer, semistrukturerade intervjuer.

4.1.2 Intervjuer

För att få svar på uppsatsens forskningsfrågor, valdes metoden semistrukturerade intervjuer som är en kvalitativ metod. Intervjuer grundas på frågor och syftar till att samla in information om respondenten. Det kan genomföras via personliga möten, telefon eller andra kommunikationsverktyg [32]. Semistrukturerade intervjuer innebär att intervjuaren förhåller sig till ett antal frågor under intervjun som bör spegla intervjun men mallen behöver inte följas strikt utan intervjuaren har möjlighet att styra intervjun.

För att komplettera vår kompetens ytterligare intervjuades Joseph Bugeja som är en forskare på Malmö Högskola som har expertis inom ämnet säkerhet i smarta hem. Valet av att intervjua denna person, grundas på att han har erfarenhet av att arbeta med säkerhetsfrågor på företag och att han forskar aktivt i ämnet. Denna intervju hjälpte oss att få mer kunskap inom ämnet som senare hjälpte oss att formulera lämpliga frågor till intervjuerna.

Vid de semistrukturerade intervjuerna användes en diktafon för att spela in samtalen. Detta gjordes för att all fokus skulle läggas på att ställa frågor och lyssna på respondenten. Båda två var närvarande vid intervjuerna, men endast en av oss agerade intervjuare. Den som inte intervjuade hanterade ljudinspelningen och ställde några få frågor i slutet som glömdes av intervjuaren. Att dela upp arbetsuppgifterna under intervjuerna bestämdes eftersom vi ansåg att det för respondenten kan uppfattas som förvirrande om det finns två som intervjuade. Dessutom ville vi inte skapa en diskussion mellan oss två och respondenten, utan hellre fokusera på att låta respondenten/respondenterna uttrycka sina personliga åsikter.

Efter intervjuerna transkiberades allt material i dokument, både frågor och svar. Varje intervju skapades i ett eget dokument för att tydligare kunna se vilken information som kunde användas i uppsatsen och för att kunna presentera resultatet med högre validitet. Frågorna markerades med fetstil för att särskilja frågorna från svaren. Efter varje fråga och svar, gjordes ett mellanrum innan nästa fråga. Utifrån frågorna och svaren som samlades in, skrevs nyckelfraser från respondenterna och nyckelfrågor som vi ansåg skulle kunna besvara våra forskningsfrågor och andra intressanta svar samt frågor. Dessa nyckelfraser

och nyckelfrågor användes sedan för att sammanställa olika tabeller för att kunna jämföra företagens svar med varandra i olika frågor. Det gav en tydligare bild av vad företagen har gemensamt och vad som skiljer dem åt. Detta gjorde att vi kunde se ett mönster i de olika svaren. Alla svar är citerade direkt från det transkiberade materialet. De finns publicerade i avsnitt 5 Resultat.

4.1.3 Litteraturstudie

För att samla mer information kring smarta hem och dess utmaningar gjordes en litteraturundersökning för att få en inblick i vilka undersökningsområden som finns inom smarta hem. Undersökningen gjordes via ACMs, IEEEs, Springers, och Google Scholars databaser. Dessa databaser publicerar selektivt ut trovärdiga forskningsarktiklar med hög standard. Böcker har använts som referenser vid metodbeskrivningen. Artiklar från dagstidningar har också använts sparsamt, för att exempelvis beskriva när system har blivit hackade och för att komplettera en del områden med ytterligare information.

För att begränsa vår sökning valdes artiklar som var under kategorier som liknade:
- "Journals/Transactions"
- "Proceedings"

Sökord som angavs för att tillgå artiklar:
- Smart homes
- Internet of Things
- Smart homes security
- Smart homes challenges
- Vulnerabilities smart homes
- Smart home architecture
- Smart homes integrity
- Security threats
- Smart home threats

4.2 Urval av företag

Vi valde att ha med fyra företag i vår undersökning, varav tre är företag som erbjuder IoT-enheter för privatpersoners bostäder. Det fjärde företaget som vi har valt att ha med i vår studie utvecklar IoT-enheter med vissa smarta hem-funktioner, såsom möjligheten att kontrollera lampor med en klocka. Företagen har välkända varumärken med stora kundkretser. För att skydda företagens anonymitet, kommer de i fortsättningen benämnas med siffrorna 1, 2, 3 och 4.

Företag	Antal personer som intervjuades	Befattning
1	Två som intervjuades tillsammans	Produktutvecklare
2	Fyra som intervjuades två och två	En mjukvaruchef, en mjukvaruarkitekt, en marknadsförare och en apputvecklare som även arbetar med cloudtjänster
3	En som intervjuades enskilt	Application Security Expert
4	Tre som intervjuades enskilt	En produktutvecklare, en IT-support och en som ansvarar för deras e-handel

Figur 4.2 Presentation av företag

Företag 1 levererar energi till företag och privatpersoner i form av bland annat el, gas, värme och kyla. Man har en tjänst som gör att man kan se och styra sin energiförbrukning i hemmet med mobilen.

Företag 2 tillverkar smarta klockor som bland annat samlar in stegdata från kunden. I framtiden kommer klockorna ha några smarta hem-funktioner såsom lampstyrning.

Företag 3 är ett företag som främst fokuserar på säkerhet i hemmet. De tillverkar flera produkter till smarta hem såsom hemlarm, lås, sensorer och övervakningskameror vilka känner av om någon går in i ditt hus. Du kan se in i ditt hus och styra lås och kameror med hjälp av en smartphone.

Företag 4 erbjuder en lösning som installeras i hemmet och som enheter sedan kopplas till. Produkter de säljer är bland annat uppkopplade markiser, rullgardiner och garageportar. Du kan även styra din energiförbrukning i mobilen och se vad som händer i ditt hus när du inte är hemma med hjälp av en övervakningskamera.

4.3 Metoddiskussion

Syftet med intervjuer är att samla in kunskap och information från respondenten [20]. Det kan anses som en lämplig metod om man till exempel vill studera en inträffad händelse, ett nyhetsfall, eller hur den anställda anser att intern information på ett företag bör hanteras. Meningen med intervjuer är att få nyanserade berättelser kring olika händelser och handlingar [20]. Intervjuer kan därför ge oss en bättre förståelse kring hur företag hanterar insamlad data, vilka utmaningar som finns med att bibehålla säkerhet och integritet för kunden vid datainsamling samt vilket ansvar företag anser att de har mot kunderna vid datahantering. Metoden tillämpas även väl för att få en utökad kunskap från experterna.

Semistrukturerade intervjuer är bra eftersom man då har ett antal frågor att förhålla sig till under intervjun och är då kompetent till att intervjua under hela intervjun [13]. Det ger också intervjuaren och respondenten frihet till att fritt uttrycka åsikter under intervjun. Semistrukturerade intervjuer kan ge trovärdig, kvalitativa data [13]. Mallen som skapas för en semistrukturerad intervju används som underlag och bör spegla vilka punkter som är viktiga att fokusera på under intervjun. Denna mall behöver inte följas strikt, utan det är respondenten som styr utvecklingen av intervjun. Under den semistrukturerade intervjun tillkommer det dessutom oftast andra uppfattningar eller idéer som ersätter eller fördjupar de punkter som redan finns i intervjumallen [25].

Personliga intervjuer lämpar sig främst när insikt kring människors personliga uppfattning sökes. Är det fler som deltar i intervjun, finns risken att respondenterna påverkas av varandras uppfattningar [20]. Till vår undersökning efterfrågade vi enskilda intervjuer med tre till fyra personer från varje företag, eftersom vi ville att de som intervjuas skulle få berätta sina egna berättelser och synpunkter utan att influeras av sina arbetskamrater. På två av företagen blev det istället att vi intervjuade två personer samtidigt. Dessa mindre gruppintervjuer bidrog till en diskussion kring hur respondenterna upplevde olika situationer. Det var även tydligt i den första intervjun att det fanns en som svarade något mer. Dock kan det ses som en fördel i att personerna var väldigt olika som personer, vilket speglade deras svar i intervjun. I boken Forskningsmetodik - Om kvalitativa och kvanitativa metoder, skriver Holme och Solvang att fokus i gruppintervjuer blir gruppens sätt

att samspela på grund av den sociala dimensionen. Vad en intervju med fler personer kan tillföra är en diskussion kring ämnet i fråga [25].

Totalt genomfördes sju intervjuer med elva personer från fyra olika företag. På grund av tidsbegränsning och storleken på vår studie valde vi att begränsa studien till fyra företag. Det ger en generell bild av hur företag arbetar, men kan inte representera hela branschen. På varje företag intervjuades personer med olika titlar som produktutvecklare och Application Security Expert. Deras befattning och arbetsuppgifter kan ha speglat svaren på något sätt. Dock representerar de i denna interjvu företaget som de arbetar på, vilket de var medvetna om. Det var dessutom företagen som valde ut de olika respondenterna till våra intervjuer.

Eftersom vi intervjuade högst två personer samtidigt, är det egentligen för få personer för att kunna kalla det en gruppintervju eller en fokusgrupp som består av fyra till tolv personer. Vissa fördelar som ofta lyfts fram för fokusgrupper kunde ändå upplevas i våra intervjuer såsom att diskussionerna som skapades byggde på respondenternas egna åsikter kring ämnet. Diskussionerna används för att utforska vilka uppfattningar och åsikter som delas i grupper samt vilka individuella tankar som finns bland deltagarna [41].

Innan vi skapade intervjuerna, utfördes som tidigare nämnt en litteraturundersökning. Detta gjorde vi för att undersöka om liknande forskning tidigare gjorts inom samma område, för att utöka vår kunskap inom hur smarta hem fungerar och ta reda på vilka säkerhetsbrister som finns i IoT-enheter. Därefter skapades två intervjumallar, en för vår expert och en för företagen. Eftersom vi valde att göra semistrukturerade intervjuer, är intervjumallen indelad i de olika kategorierna: Allmänt, Företag, Hantering av data, Företagets ansvar, Kundens ansvar, Förebyggande åtgärder och Avslut. I varje kategori finns ett antal frågor som vi utgick ifrån när vi gjorde intervjuerna. Intervjumallen som ämnades för experten hade till syfte att få hans synpunkt på vilka utmaningar som finns med säkerhet i IoT-enheter till smarta hem och vilket ansvar han tycker att företagen bör ha gentemot deras kundkrets.

Från företagen ville vi veta vilket ansvar de anser att de har mot kunderna gällande säkerhet och integritet i deras produkter och vilka säkerhetsutmaningar de upplever när de skapar dessa produkter. Dessa frågor som var utformade för företagen hade till syfte att besvara våra forskningsfrågor Q1, Q2, Q3. Gavs ett tvetydigt svar från företagen, valde vi att ställa frågan ännu en gång eller bad dem att utveckla sina svar ytterligare.

Intervjumallarna för företagen och experten hittas i avsnittet 10 Bilagor.

5 Resultat

5.1 Presentation av resultat

Nedan presenteras utvalda svar från våra intervjuundersökningar. Samtliga företags svar kring en viss fråga finns i tabeller i slutet av varje paragraf. Viss data har utvecklats i form av löpande text och citationer från intervjuerna eftersom den data är mest relevant för vår uppsats.

5.1.1 Lagring av data

Två av företagen som intervjuades lagrar all data de samlar in från sina kunder internt, det vill säga i egna databaser som endast de har tillgång till. Företag 2 skickar upp sin

kunddata till sin leverantör Amazon som lagrar den åt dem. Företag 1 använder sig av flera olika lösningar som finns både internt och externt. Produktutvecklare på Företag 1 sa:

"*Vi har ju olika lösningar och leverantörer utav cloud-lösningar. Vi har något i Värmland. Det är ganska stort. Vi har det på lite olika platser runt om i landet med olika leverantörer. Vi använder oss av båda - helt beroende på vilken typ av data det är som vi ska lagra.*"

Det är tydligt att samtliga företag i våra intervjuundersökningar samlar in all data som går att samla in. Data väljs inte selektivt ut, utan all data från deras kunder samlas in och lagras.

F01	Hur lagrar ni data?
Företag 1	Både internt och externt beroende på data
Företag 2	Amazon-instans
Företag 3	Egen databas
Företag 4	Egen databas

F02	Samlar ni in all data som går att samla in?
Företag 1	Ja
Företag 2	Ja
Företag 3	Ja
Företag 4	Ja

5.1.2 Ansvar över läckt data

De tre företagen som svarade på frågan om ansvar över läckt data var eniga om att det är företaget som bär ansvaret om data skulle läcka från deras enheter. De konstaterar att deras produkter ska vara säkra och att det är svårt att lägga ansvaret på kunden. Alla tycker det är viktigt att värna om kundernas integritet och säkerhet. Företag 2 är helt säkra på att det ligger på företaget och menar att det finns vissa personer på företaget som bär mer ansvar än andra. En mjukvaruarkitekt på Företag 2 sa:

"*Eftersom ********* är ett registrerat aktiebolag så är bolaget en juridisk instans i sig och där man håller styrelsen som den primära huvudparten. Skulle tippa på att det ligger där. Men kanske även VD har ett ansvar också.*"

Företag 1 är inte helt tydliga med att företaget bär hela ansvaret om privat data skulle läcka. De påpekar att det finns flera sätt som kunderna kan skydda sin data på. På Företag 1 sa en produktutvecklare:

"*Man får utgå att användaren gör gud vet vad som helst så man får ju göra det så säkert som möjligt. Bara en sån liten sak som att skydda sitt wifi-nätverk där hemma, det är ju inte alla som vet hur en aning om hur man gör det. Och redan där har du exponerat dig själv och allting för att någon ska kunna ta sig in för att ta sig in i ditt nätverk. Och det försöker vi förhindra med våran tjänst. Man kanske kan ta andra saker men inte ta sig in i våran tjänst. Det är svårt att lägga ansvar på användaren också.*"

F03	Vem bär ansvaret om privat data läcker? Är det företaget?
Företag 1	Företaget men användarna kan hjälpa till att skydda sin data
Företag 2	Företaget
Företag 3	Företaget
Företag 4	-

5.1.3 Utmaningar i arbetet med säkerhet och integritet

Utmaningarna som företagen ställs inför är olika. Företag 1 nämner förståelse och uppföljning av avtal som en stor utmaning. Detta nämner även Företag 3 som en utmaning. Företag 2 har ett mer specifikt problem som är kopplat till deras produkt. De vill inte att man ska kunna koppla personlig data från deras enheter till en specifik person. Detta säger de dock ska vara löst. Företag 4 ser en utmaning i att hålla koll på vem man får lov att skicka data till. Företag 3 är tydliga med vad de anser att det största problemet är och den vi intervjuade här, en Application Security Expert, beskrev deras utmaning såhär:

"*Det är att leverera en produkt som är användbar och intuitivt för kunden och samtidigt säkert. Det är två saker som har en tendens att, man vill ha ny och häftig funktionalitet men samtidigt då kunna leverera det på ett säkert sätt.*"

F04	Vilka är era största utmaningar i arbetet med säkerhet och integritet i smarta hem enheter?
Företag 1	Förståelse och uppföljning av avtal.
Företag 2	Att skilja på användaren och inte koppla personlig data till en specifik person.
Företag 3	Att leverera en användbar och intuitiv produkt som samtidigt är säker.
Företag 4	Att hålla koll på vem man får skicka data till.

5.1.4 Förebyggande arbete

Tre av de företag som vi intervjuade arbetar aktivt med att förebygga intrång och attacker på deras produkter. Detta arbete består av att göra riskanalyser och penetrationstester, antingen via företaget själv eller hyr de in från ett företag som specialiserar sig på detta. Företag 1 svarade:

"*Riskanalyser gör vi så klart. Sen testar vi grejerna jättemycket. Vi tar in externa bolag som gör penetrationstester och testar hur hårdvaran funkar, och hur vår cloudlösning funkar. De försöker ju ta sig in och hitta sårbarheter. Det här kan ni göra bättre och det här och här kan ni göra bättre. Det här måste ni ändra på. Det gör vi innan vi skickar ut det.*"

Företag 2 berättade att de har gjort en bedömning att ännu inte göra tester på deras produkter, eftersom de anser att den data som de samlar in och lagrar inte är känslig. Detta beror även på att de har en lösning som gör att det inte ska gå att se vilken data som tillhör vilken användare. En ytterligare anledning är att de litar på och anser att leverantörerna

som lagrar deras data har hög säkerhet. Däremot påpekar de att de bör göra fler tester i framtiden.

"*Vi har inte kört några tester. Vi borde ha någon test, alltså vi borde göra någonting mer. Det skulle göra oss mer konfidenta. Och det kan ju vara att man anlitar en firma också som försöker komma in åt data. Men det har vi inte idag. Så det skulle vi kunna bli bättre på.*"

F05	Hur arbetar ni för att förebygga intrång?
Företag 1	Riskanalyser och pentetrationstester
Företag 2	Inga tester utförs
Företag 3	Penetrationstester
Företag 4	Anlitar externt hackningsbolag som försöker ta sig in i systemet

5.1.5 Externa leverantörer

Samtliga fyra företag som vi har intervjuat använder sig av externa leverantörer. Antingen till lagring av data som Företag 1 och Företag 2, eller till sin hårdvara som Företag 3 och Företag 4. Eftersom Företag 1 och Företag 2 lagrar viss data hos sina leverantörer, har leverantörerna också tillgång till den. Företag 2 säger att deras leverantör lagrar deras data och använder den:

"*Nej, det är vi som måste skriva på deras avtal som det ser ut just nu. Jag läser inte dem så noga. Som Google vet jag, Firebase, de tar ju och använder datan själv ju. Så man får inte tillgång.. När man använder deras tjänst så tar de datan och får göra saker med den.*"

Företag 1 menar dock att deras leverantörer inte har rätt att varken titta på eller på annat sätt använda deras data. Så deras leverantörer har tillgång till, men inte tillstånd att på något sätt använda deras data.

"*Det finns ju en sådan personbiträdesavtal som vi har skrivit med våra leverantörer. Det är klart att de har tillgång till datan, de kan ju titta på den om de vill. Det är jättesvårt att kontrollera det.*"

Företag 3 och Företag 4 är helt säkra på att deras data bara är tillgänglig för dem själva. Båda de företagen säger att "det är vi som äger". De har inga leverantörer som de använder vid lagring av data utan lagrar den helt själva.

F06	Har ni externa leverantörer till era tjänster?
Företag 1	Ja
Företag 2	Ja
Företag 3	Ja
Företag 4	Ja

F07	Kan en tredje part ta del av insamlad data?
Företag 1	Ja, men de har inte tillstånd att göra det
Företag 2	Ja
Företag 3	Nej
Företag 4	Nej

6 Analys

I detta avsnitt väljs vissa delar ut från resultatet och analyseras. Detta innebär att några av företagen analyseras mer i detta avsnitt än andra. Hela resultatet finns i avsnitt 5.

6.1 Lagring av data

Svaren till frågan *"Hur lagrar ni data?"* besvarar forskningsfrågan Q2. Alla företag lagrar sin insamlade data med hjälp av en molnlösning som antingen sköts av företagen själva eller via en extern leverantör. Tre av företagen väljer att ha en egen molnlösning. De har en intern databas som endast de har tillgång till. Företag 1 har utöver sin interna lösning valt att ha en extern molnlösning som inte sköts av dem själva. Var den data som samlas in sedan lagras beror på hur känslig den är. Vad de definierar som känslig data är oklart och det kan diskuteras vem som bestämmer om data är känslig eller inte. Företag 2 skickar upp sin insamlade användardata till Amazons servrar som lagrar data till dem. Detta innebär att de inte har kontroll över sin data och äger den inte.

De två företagen som endast använder sig av intern molnlagring har ständig kontroll över all data från deras kunder. De har full kontroll och kan försäkra sig om att molnlagringen lever upp till de säkerhetskrav som finns och hanteras på rätt sätt. I Företag 4 lagras all data i en egen molnlösning som finns i ett annat europeiskt land. Detta kan skapa problem eftersom olika länder har olika regler och det blir därför svårare att hålla koll på vad som gäller i vilket land. Företag 2 använder också Googles Firebase för analysering av data, och förklarar att de skriver på avtal med Google Firebase vilket ger Google rättigheter att använda denna data. Om företaget eller företagets kunder vill ta tillbaka den rådata som har samlats in, måste företaget betala för det.

Alla fyra företag samlar in all data som går att samla in från kunderna. Detta innebär att all data som går att tillgå från kunderna samlas in och lagras, utan sortering.

6.2 Ansvar över läckt data

Tre av företagen var överens om att det är de som bör ta på sig ansvaret om det skulle läcka data från deras produkter. Till Företag 4 ställdes aldrig denna fråga eftersom intervjun tog en annan riktning och vissa frågor inte hann ställas. De tre företagen som fick frågan menade alla att det skulle vara deras fel om kunder skulle upptäcka att någon har gjort intrång i deras produkter. Företag 2 reflekterade inte ens över kundens roll vid en sådan händelse utan började diskutera om vilka på företaget som har det största ansvaret. Även Företag 1 och Företag 3 var tydliga med att det främst är företaget som ska stå för säkerheten, men Företag 1 nämner även kundens roll. De anser att det finns flera saker som kunderna själva kan göra för att höja säkerheten i produkterna. Kanske kan denna

övertygelse bland företagen tolkas som att kunden kan lite på företag fullt ut. Dock bör det bli tydligare, som Företag 1 nämnde, att även kunden kan göra sina produkter säkrare. Kundens roll upplevs inte alls lika viktig i denna situationen utan fokus ligger på företaget vilket kan ifrågasättas.

6.3 Förebyggande säkerhetsarbete

De företag som vi har intervjuat arbetar lite olika för att förebygga intrång i sina system. Företag 2 säger att de aldrig har testat sitt system över huvud taget men påpekar att det vore en bra idé. Att ett företag inte testar sina produkter alls kan vara ett problem eftersom de då inte är medvetna om systemets brister. Om kunderna till detta företag skulle bli medvetna om detta skulle de kanske tappa kunder eftersom systemet då upplevs som osäkert. Företag 4 utför regelbundet riskanalyser och gör mycket penetrationstestning för att hitta sårbarheter i systemet. Detta är en självklarhet för dem eftersom de vill ha ett så säkert system som möjligt. Även Företag 3 penetrationstestar regelbundet med hjälp av olika testare för att förebygga intrång. Företag 4 anlitar kontinuerligt ett externt hackningsbolag med testare som försöker hacka sig in i systemet och har således blivit certifierade av dem.

De tre företag som regelbundet testar sina system arbetar med det på lite olika sätt även om de alla penetrationstestar. Företag 1 jobbar både med riskanalyser och penetrationstester medan Företag 3 nöjer sig med interna penetrationstester. Även Företag 4 penetrationstestar sina system, men de anlitar ett externt hackningsbolag som utför det åt dem. Trots att de tre företagen har olika tillvägagångssätt i sin testning finns det likheter och samtliga utför det i samma syfte; att skapa ett så säkert system som möjligt.

6.4 Lagar och regler

I våra intervjuer påpekade flera personer att lagar skiljer sig åt beroende på vilket land produkten säljs i. Eftersom det kommer en ny lag från EU i maj 2018, Dataskyddsreformen [14], så kommer företagen som vi har intervjuat behöva anpassa sig efter den. Flera av företagen kände till detta direktiv. Företag 2 var det företag som i nuläget arbetar fram en lösning som täcker det nya direktivet. Dock var ingen av de vi intervjuade någon som arbetade mycket med detta utan de har andra kollegor som hanterar dessa juridiska frågor. På grund av detta var ingen speciellt insatt i hur företaget kommer hantera dessa förändringar. De flesta respondenterna nämnde att företag är tvungen att ta hänsyn till varje lands egna regler trots att det finns gemensamma regler för hela EU, eftersom dessa kan skilja sig åt. Även om de följer det nya EU-direktivet till fullo kommer de vara tvungna att kontrollera varje lands egna regler vilket är kostsamt men nödvändigt. Det kan då ifrågasättas hur kunders data hanteras och lagras utav de olika företagen som har externa leverantörer och molntjänster som är belägna i andra EU-länder, e+ftersom de inte kan garantera att data hanteras och lagras med samma riktlinjer som i Sverige.

6.5 Leverantörer och dess tillgång

Det visade sig att samtliga företag som vi pratade med samarbetar med externa leverantörer till sina tjänster och produkter. Alla tre företag som säljer produkter till smarta hem

använder sig av leverantörer till sin hårdvara, exempelvis kameror, brandlarm, termometer och det centrala systemet. Företag 2 tillverkar sina klockor själva men använder sig av andra företags tjänster för bland annat datalagring. Samtliga företag påpekar att den data som samlas in från kunderna inte kan och får användas av deras leverantörer. Två av företagen säger att deras leverantörer faktiskt kan tillgå data som de har samlat in, men av rättighetsskäl får de inte ta del av den. Dessa två företag säger dock att man inte kontrollerar om leverantörerna på något sätt använder deras data eftersom det är svårt att kontrollera. Att obehöriga, tredje parter faktiskt har tillgång till och kan använda data bland hälften av de intervjuade företagen kan upplevas som mycket problematiskt. Även om leverantörerna inte får använda datan, har de tillgång till den och om de skulle ta del av den skulle inte företagen märka det.

7 Diskussion

I detta avsnitt diskuteras punkter som har lyfts fram i Resultat och Analys, som bland annat svarar på de tre frågeställningarna.

7.1 Lagring av data

Tre av de företag som vi har intervjuat använder sig av egna databaser där de lagrar data som de samlat in från sina kunder. Säkerheten i sådana här kan tyckas vara högre än att lagra sin data från sina kunder på andras servrar, såsom Googles eller Amazons, som Företag 2 gör. Vad som kan uppfattas som problematiskt med att lagra data hos andra leverantörer, såsom Företag 2 gör, är att företaget förlorar full kontroll över hur denna data hanteras. När vi pratade med Företag 2 påstår de att deras leverantörer absolut har tillgång till deras kunddata. För en kund kan det kännas olustigt att fler än företaget har tillgång till deras data. Detta är dock en ekonomisk fråga eftersom det är dyrare att upprätthålla en server på egen hand. Även när data lagras i ett annat land, kan datahanteringen påverkas mer. Detta beror på att alla enskilda länder i Europa har egna regler och tillämpningar för hur data får hanteras och brukas, vilket inte alltid stämmer överens med de gemensamma reglerna. Företag 4, exempelvis, är ett företag som inte är svenskt och de lagrar all sin data i ett annat EU-land. Detta kan påverka deras sätt att hantera och använda den data de samlar in.

Det nya direktivet från EU som tillträder nästa år, ger konsumenterna rätten till att ta bort data som har samlats in utav företagen. Företagens samarbete med dessa leverantörer kan då komma att påverkas, då nya avtal förmodligen måste skrivas om för att företagen ska kunna kräva detta. I nuläget kan vissa leverantörer såsom Amazon och Firebase (beroende på hur det står i avtal), använda den data som lagras och samlas in. För att företaget ska kunna ta bort den data som har samlats in måste företaget betala en summa.

Det kan diskuteras om företaget själva bör hantera lagring av data eller om de bör distribuera detta till en leverantör. Fördelar med att ha leverantörer är att det är billigare eftersom företaget inte behöver tillhandhålla och underhålla servrar och databaser för detta, och de behöver inte heller anlita personal för detta. Däremot förlorar de kontrollen över data, även om avtal skrivs med leverantörerna. Företag 1 och Företag 2, som lagrar data hos en annan leverantör, har gjort en bedömning på den data de väljer att lagra hos andra.

De prioriterar datans känslighet. Om data är mindre känslig, till exempel data som säger hur många steg en användare gått per dag, väljer de att lagra den hos en leverantör.

7.2 Utmaningar med avtal

När företagen fick frågan om deras främst utmaningar i säkerhetsarbetet var det väldigt olika svar. Dock framkom det i samtliga intervjuer en svårighet kring avtal. En utmaning som samtliga företag nämner någon gång i respektive intervju är att förstå och kontrollera avtal. Företag 1 och Företag 2 har båda leverantörer som har tillgång till data som samlas in från företagens kunder. Detta visas i Resultatet, tabell F07. Företag 1 har skrivit avtal mellan sig och leverantören som säger att leverantören inte får titta på eller använda data i något syfte. Företaget säger dock att detta inte följs upp på något sätt och att det är mycket svårt att kontrollera. Företag 2 påstår sig vara säkra på att Google använder deras data, men verkar inte se det som ett problem. Att leverantörer till företag som samlar in data har tillgång till deras kunddata kan vara ett problem och vi tror att det är något som kunderna inte är medvetna om. Detta eftersom samtliga företag upplevde att kunderna inte läste användaravtal vid köp av produkt.

På grund av att många kunder förmodligen inte är medvetna om vad som står i användaravtal, kan det diskuteras om hur man kan få dem att läsa dessa. Användare bör förstå hur viktiga användarvillkor är. Genom att godkänna användarvillkor ger man ett företag möjligheten att hantera data på ett sätt som man kanske inte är medveten om. Ofta är avtalet långt, formellt skrivet och består av flera tekniska termer vilket leder till att kunden inte läser det. Många struntar också i att läsa det eftersom de litar på företaget. Användare måste dock förstå att man godkänner flera saker när man skriver på ett användaravtal. Kanske kan man göra avtalen enklare att läsa genom att undvika att skriva det formellt och korta ner dem så att flera orkar läsa det. För att nå fler människor kan man ta med det viktigaste och skriva det på ett lättläst sätt så att det blir fler människor som förstår vad avtalet innebär. Det bör dock finnas en längre version som tar med allt som gäller med avtalet.

7.3 Företagens och kundernas ansvar

Som nämnt i avsnittet 3.4 Relaterade studier, menar Alan Grau [24] på att företaget främst står för säkerheten i produkter till smarta hem. Han påpekar dock att användarna själva kan vara med och öka säkerheten på olika sätt. I denna fråga är både Grau och samtliga företag som vi har ställt frågan till överens.

Alla tre företag som fick frågan var överens om att det är företagets ansvar om data skulle läcka från deras produkter. Det är de som bygger produkterna som kunderna sedan använder. Därför anser de att produkterna måste hålla hög kvalité gällande säkerhet och skydda den data som de samlar in på ett sätt så att andra inte kan kan ta del av datan. Detta skulle kunna tolkas som att kunderna kan lite på företaget fullt ut.

Företag 1 var det företag som lyfte fram kundens roll i denna situation. De beskrev flera saker som kunden själv kan göra för att förbättra säkerheten i sina produkter. Bland annat kan man byta lösenord ofta och vara noga med att uppdatera produkterna. Dock sa dem att kunderna ofta inte är medvetna om detta och att de inte vet vad de kan göra för att förebygga intrång. Detta är något som företagen kan vara bättra på att förmedla till sina kunder.

Som kund har du ett ansvar över att inte förenkla processen för obehöriga att tillgå data från dina produkter. Något som tidigare nämnts i denna uppsats, är David Jacoby som hackade sig in på sina egna smarta hem-produkter. Han nämnde att människor inte är lika duktiga på att göra säkerhetsuppdateringar på sina smarta hem-produkter som med sina datorer, vilket är kundens ansvar. Han ger dessutom exempel på hur kunder kan skydda sina produkter från intrång. Genom att ändra det förinställda lösenordet på produkterna och ändra sina inställningar på routern så att varje produkt får ett eget nätverk gör att produkterna blir säkrare [30].

Alla kunder vill förmodligen ha så hög säkerhet som möjligt och om de får veta vad de kan göra för att säkra sina produkter, skulle de nog vara villiga att göra det. Företaget och dess kunder bör samarbeta och kommunicera kring säkerhetsfrågor för att uppnå bästa möjliga säkerhet.

7.4 Känslig data

De fyra företagen som vi har intervjuat samlar in olika typer av data. Företag 1 samlar in data kring energi- och elförbrukning. Företag 2 samlar bland annat in hur många steg användaren gått under dagen och när du trycker igång play eller pause för musik. Företag 3 samlar in data kring om någon obehörig är i ditt hem, när du låser dörren och om det finns möss. Företag 4 samlar bland annat in data om när du tänder och släcker dina lampor och när du drar ner dina rullgardiner. Som visas nedan anser varken Företag 1 eller Företag 2 att de lagrar känslig data.

Företag 1: *"...den är så inte så känslig som, du har ju dataförsvarets anläggningar också ju, och den är klassad på ett annat sätt."*
Företag 2: *"...det är ingen känslig, det är ingen bankinloggning eller..."*

Det kan diskuteras om den data dessa två företag samlar in verkligen inte är känslig. Olika användare kan anse att stegdata är känslig medan andra gärna lämnar ut vilken data som helst till vem som helst. Det är svårt att definiera känslig data eftersom det skiljer sig från person till person. Som Företag 1 påpekar finns det data som är betydligt mer känslig men för vissa personer kan information om dess energiförbrukning vara minst lika känslig, eftersom det kan visa på när personen är hemma och inte.

7.5 Trovärdighet

Golle [22] är i sin artikel tydlig med att hur företag hanterar data är viktigt för trovärdigheten. Han menar att privatpersoner är mer belägna att lämna ut sin data till ett företag som har hög säkerhet och bevarar integriteten. Detta bör företag som samlar in och lagrar data vara medvetna om. Företag 2 använder Amazon för sin lagring av kunddata. De utför inga tester på sina produkter, vilket kan tyda på mindre säkerhet. Detta kan ge dem mindre trovärdighet, då regelbudna tester kan öka produktens säkerheten. Dock använder de sig av anonymisering, man kan inte koppla ihop känslig data med en individuell identitet. Trots att de har anonymisering bör man testa sitt system för att hitta svagheter och hot.

7.6 Dilemmat med säkerhet

Dilemmat med säkerhet, som vi skrev om i avsnitt 3.2, är ett fenomen som vi har förstått visar sig bland riktiga företag. Företag 3 påpekar detta i sin intervju. De tycker deras största utmaning är att *"leverera en produkt som är användbar och intuitivt för kunden och samtidigt säkert"*. Det är en balansgång i arbetet med att ta fram nya produkter och samtidgt lägga resurser på säkerhetsarbete. Som företag behöver man överväga hur mycket man kan kompensera det ena med det andra. Som ovan nämnt har kunder vissa krav på vilken säkerhet de vill ha som de kan ha svårigheter att uttrycka. Samtidigt krävs ny och häftig funktionalitet i samband med snabb leverans. Utan att kunna uttrycka den säkerhet som kunder kräver, läggs därför ett indirekt ansvar på företag att inte missbruka kundernas okunskap. Att prioritera säkerhet har dessutom andra faktorer som kan avgöra företagens val av hur mycket säkerhet som implementeras i deras produkter, såsom resurser och kunskap i vilken säkerhet som krävs. Vid utveckling av produkter krävs testning för att företagens ska kunna försäkra sig om att data hanteras på rätt sätt och att någon som inte är behörig får tillgång till denna data. Detta kräver resurser. Denna kunskap och insikt samt resurser kan tänkas saknas hos start-ups, som är ett ord för nystartade företag, där funktionalitet och snabb leverans kan prioriteras framför säkerhet.

7.7 Förbättringsmöjligheter

Utifrån våra resultat vill vi rekommendera privatpersoner som har IoT-enheter i sitt hem eller som funderar på att köpa det, att läsa avtalen som skrivs med företagen för att bli mer medveten kring vilken data som samlas in och hur denna används. Kunder bör även kunna ställa krav på dessa avtal, de ska vara lättlästa samt vara en rimlig längd. De företag som vi valde att intervjua är väletablerade och arbetar aktivt med säkerhetsfrågor. Det finns säkerligen företag som inte håller samma standard och som inte prioriterar säkerhet lika mycket som att implementera häftig funktionalitet. Vad som också kan skilja är hur data hanteras beroende på vilket land företaget befinner sig i. Gäller detta EU finns det EU-direktiv som företag måste förhålla sig till, trots detta finns det vissa skillnader mellan de olika länderna. Ligger företaget utanför Europa, bör man som kund förslagsvis undersöka företaget och ställa frågor för att försäkra sig om att man köper en säker produkt samt att den data som samlas in hålls inom företaget. Dessvärre förväntas det idag att konsumenten är kunnig kring teknik och kan ställa rätt frågor kring säkerhet på egen hand, vilket innebär att kunden själv måste vara aktiv i dessa frågor.

Vad som kan rekommenderas för företag är att påskrivna avtal med andra leverantörer såsom molntjänster följs upp och att företagen undersöker vad som faktiskt händer med den data som de lagrar där. Lika väl som att företagens kunder kan ställa krav på företag som säljer IoT-enheter till smarta hem, bör även dessa företag kunna ställa krav på sina leverantörer. Företagen har dessutom ett ansvar att läsa och veta vad dessa avtal innebär. Om dessa leverantörer finns i andra EU-länder kan detta innebära att de hanterar data på ett annat sätt och med andra regler. En lösning för detta kan vara att starta en molnlösning i Sverige, och följa svenska lagar samt de direktiv som finns från EU. Dessutom bör företagen försäkra sig om att deras personal som säljer smarta hem-enheterna bör ha viss kunskap kring vilken data som lagras och hur den lagras för att kunna svara på kunders eventuella frågor.

8 Slutsatser och vidare forskning

Efter att ha utfört intervjuerna kan vi fastställa att företagen upplever olika utmaningar vid insamling av data och med att bibehålla säkerhet och integritet för kunderna. En utmaning som är återkommande är förståelse av avtal. Avtal uppfattas ofta som långa och tråkiga vilket leder till att få läser och förstår dem. Detta gäller både avtal mellan företag och leverantör och mellan företag och kund.

En slutsats som kan dras är att det kan upplevas som svårare att ha kontroll över vad som händer med datan vid lagring hos en extern molntjänst. Detta beror på att företaget lämnar över ansvaret till en annan leverantör och i vissa fall för att molntjänsten ligger i ett annat europeiskt land. Trots att Europa har lagar för hur data får lagras, så finns det även skillnader hos olika länder. Detta upplevs som en av svårigheterna. För vidare forskning kan man även undersöka om, och i så fall hur, data hos leverantörer till företagen används. Även om man skriver avtal med leverantörer kontrolleras det inte hurvida de tar del av data eller inte. Hur detta kan kontrolleras skulle kunna utforskas.

Hur företag lagrar data beror mycket på vad det är för data som samlas in och man bör även ta hänsyn till den ekonomiska aspekten. Det är dyrare att upprätthålla en server på egen hand. Därför skulle det vara intressant att undersöka om säkerheten och sättet att lagra data på skiljer sig mellan nyetablerade, mindre företag och större företag som har funnits på marknaden ett tag. I denna undersökning har vi valt att ha med tre väletablerade företag och ett relativt nytt men som grundar sig från ett annat välkänt företag. Detta kan ha påverkat våra resultat eftersom större företag oftast har mer resurser att spendera på säkerhet och de är medvetna om att det är viktigt att investera i säkerheten på deras produkter.

En annan sak som företagen var överens om var att hur skyddad data bör vara helt beror på dess känslighet. Är det exempelvis kontokortsuppgifter eller personuppgifter, kräver detta högre säkerhet än data som talar om hur många steg en användare har gått per dag. Det kan dock uppfattas som problematiskt eftersom känslig data kan uppfattas olika för olika människor. Företag bör lägga mer resurser på säkerhet av all data eftersom viss data kan uppfattas som känslig för en viss person.

Utifrån resultatet är det väldigt tydligt att företaget bär ansvaret om data läcker från deras produkter. Det kan uppfattas som att privatpersoner kan lita på företag som säljer IoT-produkter till smarta hem och inte själva behöver tänka på säkerheten. Detta upplever vi som problematiskt eftersom högsta säkerhet uppnås om flera parter samarbetar i säkerhetsarbetet. Företagen bör vara tydligare med att berätta för sina kunder hur de själva kan förbättra säkerheten, eftersom det inte görs i någon större utsträckning idag. Detta leder också till en omedvetenhet bland kunder. Något som skulle vara intressant att undersöka vidare är kundernas perspektiv på datahantering av företag. Kundernas medvetenhet kring detta är ett område som skulle kunna ifrågasättas. Många kunder är inte medvetna om hur data från dem lagras och hanteras, denna medvetenhet bör kunna bli större.

Referenser

[1] Al-Fuqaha, Ala, Guizani, Mohsen, Mohammadi, Mehdi, Aledhari, Mohammed and Ayyash Moussa. 2015. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. *IEEE Communications Surveys and Tutorials* 17 (4): 2347-2376.

[2] Badica, Costin, Brezovan, Marius, Badica, Amelia. 2013. An Overview of Smart Home Environments: Architectures, Technologies and Applications. http://ceur-ws.org/Vol-1036/p78-Badica.pdf (Hämtad 2017-03-02).

[3] Barclays. *Five killer reasons to use cloud storage.* http://www.barclays.co.uk/Startupsupport/Five-killer-reasons-to-use-cloud-storage (Hämtad 2017-03-13).

[4] Bates, Oliver, Friday, Adrian. 2017. Beyond Data in the Smart City: Repurposing Existing Campus IoT. *IEEE Pervasive Computing* 16 (2): 54-60. doi: 10.1109/MPRV.2017.30

[5] Beligianni, Foteini, Alamaniotis, Militadis, Fevgas, Athanasios, Tsompanopoulou, Panagiota, Panayiotis, Bozanis and Tsoukalas, Lefteri H. 2016. An internet of things architecture for preserving privacy of energy consumption. *Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion* 1-7. doi: 10.1049/cp.2016.1096

[6] Bertino, Elisa. 2016. Data Security and Privacy in the IoT. *Keynote Summary, Proceedings of EDBT 2016.*

[7] Bertino, Elisa, Choo, Raymond Kim-Kwang, Georgakopolous, Dimitrios och Nepal, Surya. 2016. Internet of Things (IoT): Smart and Secure Service Delivery. *ACM Transactions on Internet Technology (TOIT) - Special Issue on Internet of Things (IoT): Smart and Secure Service Delivery* 16(4) Article No 24.

[8] Bugeja, Joseph, Jacobsson, Andreas och Davidsson, Paul. 2016. On Privacy and Security Challenges in Smart Connected Homes. *Intelligence and Security Informatics Conference (EISIC), 2016 European:* 172-175. doi: 10.1109/EISIC.2016.044

[9] Carlsson, Bengt och Jacobsson, Andreas. 2012. *Om säkerhet i digitala ekosystem.* 1. upp. Lund: Studentlitteratur.

[10] Carlsson, Bertil. 1991. *Kvalitativa forskningsmetoder - För medicin och beteendevetenskap.* 1. uppl. Falköping: Gummessons Tryckeri AB.

[11] Chan, Marie, Campo, Eric, Estève, Daniel och Fourniols, Jean-Yves. 2009. Smart homes - current features and future perspectives. *Maturitas* 64 (2): 90-97.

[12] Cnet. 2017. *Best Smart Home Devices of 2017.* https://www.cnet.com/topics/smart-home/best-smart-home-devices/ (Hämtad 2017-03-02).

[13] Cohen D, Crabtree B. 2006. *Qualitative Research Guidelines Project.* http://www.qualres.org/HomeSemi-3629.html (Hämtad 2017-03-06).

[14] Datainspektionen. *Dataskyddsreformen.* http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/ (Hämtad: 2017-03-09)

[15] Datainspektionen. *Personuppgiftslagen.* http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/ (Hämtad: 2017-03-09)

[16] Datainspektionen. 2017. *Introduktion till dataskyddsförordningen.* http://www.datainspektionen.se/dataskyddsreformen/ dataskyddsforordningen/dataskyddsdagen/ (Hämtad 2017-03-13).

[17] Delaney, R. John. 2017. *The Best Smart Home Security Systems of 2017.* PCMag UK. http://uk.pcmag.com/surveillance-cameras/74995/guide/the-best-smart-home-security-systems-of-2017 (Hämtad 2017-03-02).

[18] Devi Niranjana, K och Muthuselvi, R. 2016. Parallell processing of IoT health care applications. *Intelligent Systems and Control (ISCO).*

[19] Dictionairy.com. *Privacy.* http://www.dictionary.com/browse/privacy (Hämtad 2017-03-13).

[20] Ekström, Mats och Larsson Larsäke. 2000. *Metoder i kommunikationsvetenskap.* 1. uppl. Lund: Studentlitteratur.

[21] Elmered, Peter. 2013. ZigBee vs. Z-Wave – Teknikerna inom hemautomatisering som du bör ha koll på. *Homeautomate.it.* http://homeautomateit.com/standarder/zigbee-vs-z-wave-teknikerna-inom-hemautomatisering-som-du-bor-ha-koll-pa/ (Hämtad 2017-03-07).

[22] Golle, Philippe, McSherry, Frank och Mironov, Ilya. 2008. Data Collection with Self-Enforcing Privacy. *ACM Transactions on Information and System Security (TISSEC)* 12 (9). doi: 10.1145/1455518.1455521

[23] Gollmann, Dieter. 2011. *Computer security.* 3rd edition. Chichester: John Wiley Sons Ltd.

[24] Grau, Alan. 2017. *Security for the Smart Home - Who is Responsible?* Icon Labs. http://www.iconlabs.com/prod/security-smart-home-

[25] Holme, Idar Magne och Solvang, Bernt Krohn. 2001. *Forskningsmetodik - Om kvalitativa och kvantitativa metoder.* 2. uppl. Lund: Studentlitteratur.

[26] Internet of Things Sverige. 2017. *Om IoT.* https://iotsverige.se/internet-things-2/ (H mtad 2017-03-23).

[27] Kumar, Pardeep, Braeken, An, Gurtov, Andrei, Linatti, Jari and Ha Hoai Phuong. 2017. Anonymous Secure Framework in Connected Smart Home Enviroments. *IEEE Transactions on Information Forensics and Security* 12(4): 968 - 979.

[28] Lamonica, Martin. 2014. Will smart home technology systems make consumers more energy efficient? *The Guardian.* https://www.theguardian.com/sustainable-business/smart-home-technology-energy-nest-automation (Hämtad 2017-03-02).

[29] Liao, Chun-Feng. 2017. A Formal Model for Robust Spatial-Aware Service Management in IoT-enriched Smart Home. *International Conference on Platform Technology and Service (PlatCon):* 1-6. doi: 10.1109/PlatCon.2017.7883676

[30] Malmgren, Kim. 2014. David Jacoby hackade sin hemelektronik. *Expressen.* 21 augusti. http://www.expressen.se/nyheter/david-jacoby-hackade-sin-hemelektronik/ (Hämtad: 2017-03-29).

[31] Manikandan, J. 2016. Design and evaluation of wireless home automation systems. *2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES):* 1-5. doi: 10.1109/ICPEICES.2016.7853323

[32] Patel, Runa och Davidson, Bo. 2003. *Forskningsmetodikens grunder - Att planera, genomföra och rapportera en undersökning.* 3. uppl. Lund: Studentlitteratur.

[33] Piktochart. https://piktochart.com/

[34] Ransing, S. Sarika, Rajput, Manita. 2015. Smart Home for Elderly Care, based on Wireless Sensor Network. *Nascent Technologies in the Engineering Field (ICNTE).* doi: 10.1109/ICNTE.2015.7029932.

[35] Ruj, Sushmita, Stojmenovic Milos och Nayak, Amiya. 2012. Privacy Preserving Access Control with Authentication for Securing Data in Clouds. *CCGRID '12 Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.* pp. 556-563. doi: 10.1109/CCGrid.2012.92.

[36] Siboni, Shachar, Shabtai, Asaf, Tippenhauer, Nils O., Lee, Jamin, Elovici, Yuval. 2016. Advanced Security Testbed Framework for Wearable IoT Devices. *ACM Transactions on Internet Technology (TOIT) - Special Issue on Internet of Things (IoT): Smart and Secure Service Delivery* 16(4) Article No 26.

[37] Statens Medicinsk-Etiska Räd. *Integritet.* http://www.smer.se/etik/integritet/ (Hämtad 2017-03-09).

[38] Stålbröst, Mats. 2009. 35 molntjänster som får ditt företag att lätta. *InternetWorld.* http://internetworld.idg.se/2.1006/1.205521/35-molntjanster-som-far-ditt-foretag-att-latta (Hämtad 2017-03-07).

[39] Sundling, Janne. 2015. Smarta hem ger nya möjligheter. *Dagens samhälle.* 12 februari. https://www.sics.se/sites/default/files/pub/swedishict.se/smarta_hem.pdf (Hämtad 2017-02-21).

[40] Svenska Akademiens ordlista. *Integritet.* http://www2.svenskaakademien.se/svenska_spraket/svenska_akademiens_ordlista/saol_13_pa_natet/ordlista (Hämtad 2017-03-09).

[41] Tong, Allison, Sainsbury, Peter och Craig, Jonathan. 2007. Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups. *International Journal for Quality in Health Care* 19 (6): 349-357. doi: https://doi.org/10.1093/intqhc/mzm042 (Hämtad 2017-03-10).

[42] TT. 2017. Smarta hem öppnar upp för virus. *Dagens Industri.* 14 januari. http://www.di.se/nyheter/smarta-hem-oppnar-upp-for-virus/ (Hämtad: 2017-03-29).

[43] Örstadius, Kristoffer. 2016. Expert: Kamerornas säkerhet är undermålig. *Dagens Nyheter.* 22 maj. http://www.dn.se/nyheter/expert-kamerornas-sakerhet-ar-undermalig/ (Hämtad: 2017-03-29).

9 Bilagor

Nedan visas hur våra intervjumallar såg ut inför våra intervjuer. Intervjun med experten hölls på engelska eftersom den vi intervjuade inte pratar svenska utan främst engelska. Samtliga intervjuer med företagen hölls på svenska.

9.1 Intervjumall för experten

General
Name:

What year were you born?

Profession:

Background in Computer Science:

What are you researching now?

When did your interest for security in Computer Science start?

Do you own smart home products?
-From which company?

Smart homes in general
What is the definition of smart homes?

What are the advantages with smart homes?

What are the disadvantages with smart homes?

In what ways are smart home devices vulnerable to security threats? If so why?

In what way can a smart home user be affected of security risks without knowing it?

Are some attacks more common in Smart homes than others? Which ones?

Are there laws that protect smart home users in Sweden?
- Even if they are being hacked from different countries?

How can different laws in different countries make it more complex to use laws to protect the user?

Companies
Have you helped companies improve their security for their customers before?

Do you think the customers rely too much on companies to make sure that the smart home devices are secure?

What challenges do you think companies face today regarding securing their customers integrity?

What do you think are the biggest flaws in companies in their work with security and integrity in smart homes?

What can companies do to improve users integrity in smart homes?

How should companies handle gathered data from the users in your opinion?

What responsibility should the companies that sell Smart home devices have of users integrity in your opinion?

Do you also feel that suppliers of the product have responsibility in this?

Who is to blame if gather data from the companies under has leaked, is the company or the person?
- Could this be investigated?

Not much security scandals has been published in the newspapers or the tv news, do you think the companies handle it internally to avoid damage to their brand?

Do you know if there are any laws that protect customers from unauthorized people taking private data that is collected from smart homes?

User
What responsibility do smart home users have for their own integrity and security in your opinion?

How can users improve security on their own?

How much of attacks and sharing of gathered data are the users aware of, do you think?

Can the users trust the companies that sell Smart home devices?

Do you think that there is a difference if you buy it from a big well known company or small company?

9.2 Intervjumall för företag

Allmänt
Företag:

Namn:

Befattning/titel:

Arbetsuppgifter:

Hur länge har du jobbat på företaget?

Vad har du jobbat med tidigare?

När började ditt intresse för att arbeta med datorer?

Hur många arbetar med säkerhets- och integritetsfrågor för kunder på din arbetsplats?

Företaget
När började ni utveckla smarta hem produkter?

Kan du beskriva några smarta hem produkter ni säljer och hur de fungerar?

Kan smarta hem enheternas säkerhet skilja sig beroende på prisklass?
- Varför?

Köper ni in produkter från andra leverantörer eller är det något som ni i företaget tillverkar?

Isåfall, Vilka delar tillverkar/ hanterar leverantörer till era enheter?

Hantering av data
Hur hanterar ni data som samlas in från enheterna?

Finns det tredje parter som kan ta del av data?

Om ni har delar från leverantörer, kan de ta del av data som samlas in?

Var samlar ni data?
- Lagrar ni data internt eller externt?
- Lagrar ni via en molnlösning?

Finns det lagar som skyddar kunderna från obehöriga personer att tillgå data som samlas in från smarta hem enheter?

Har ni eller kunder upptäckt att det finns personer utifrån som inte tillhör företaget som försöker ta del av data som samlats in av era enheter?

Hur hanterar ni detta?

Hur förebygger ni det?

Vid brott, får ni ge ut data som samlats in från era användare till polis?

Företagets ansvar
Vilka är era största utmaningar i arbetet med säkerhet och integritet i smarta hem enheter?

Vilket ansvar anser du att ni som företag har över era kunders integritet i smarta hem?
- Varför?

Har leverantörerna något ansvar över era kunders integritet i smarta hem?

Inkommer det många situationer då era kunder har upplevt säkerhetsbrister i hur data som samlats in har hanterats?
- Beskriv en sådan situation?
- Hur har osäkerheten uppstått?
- Vems ansvar är det?
- Hur har ni som företag agerat i en sådan situation?

Kundens ansvar
Vilket ansvar anser du att era kunder själva har för sin integritet i smarta hem?

Är privatpersoner medvetna om sitt eget ansvar?

Förlitar sig kunderna på företagen att säkerheten är på topp?

Förebyggande åtgärder
Hur arbetar ni för att förbättra säkerheten för kundernas integritet på smarta hem enheterna ni säljer?

Avslut
Har ni gjort någon undersökning om hur kundernas nöjdhet med sin säkerhet med era varor?
- Vad har det gett er?
- Går det att få tillgång till dem?

Är det okej om vi kontaktar dig igen om vi har några ytterligare frågor och funderingar?