LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Säkerhetsbrister med Internet of Things

En studie om företags upplevelser av säkerhetsbrister

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Victoria Andersson
Emma Nilsson
Matilda Stading

Handledare: Miranda Kajtazi

Examinatorer: Anders Svensson
Nicklas Holmberg

Säkerhetsbrister med Internet of Things: En studie om företags upplevelser av säkerhetsbrister

Författare: Victoria Andersson, Emma Nilsson och Matilda Stading

Utgivare: Inst. för informatik, Ekonomihögskolan, Lunds universitet

Framlagd: maj, 2018

Dokumenttyp: Kandidatuppsats

Antal sidor: 84

Nyckelord: Internet of Things, IoT, IoT-infrastruktur, säkerhetsbrister, CIA, säkerhet, privacy, medvetenhet

Sammanfattning (Max. 200 ord):

Fenomenet Internet of Things (IoT) har ökat exponentiellt de senaste åren, och är idag ett av de mest diskuterade ämnena inom IT-branschen. Vardagliga enheter som lampor, alarm, övervakningskameror går numera att koppla upp till molntjänster för att underlätta livet för både företag och individer. Precis som vilken annan uppkopplad enhet, så medföljer flera säkerhetsbrister, vilket innebär att omedvetna och okunniga företag riskerar att utsättas för intrång på olika nivåer. Just på grund av den stora tillväxten av IoT-enheter hinner inte utvecklingen av säkerheten med eller också blir den bortprioriterad. Istället prioriteras funktion och design. Denna svaghet har på senaste uppmärksammats mer, och kan användas nu också för att stjäla information. Genom en kvalitativ studie med aktörer inom IT-branschen tillsammans med litteratur undersöks det vilka faktorer som bidrar till säkerhetsbrister. Studien har resulterat i att resursbrist, mängd enheter och medvetenhet är faktorer som bidrar till att många företag prioriterar andra saker framför säkerhet.

1 Innehåll

2 Figurer

3 Tabeller

4. Ordlista

IoT	Internet of Things
Web 1.0	Första versionen av World Wide Web
Web 4.0	Nästa generation av World Wide Web
RFID	Radio-frequency identification
CEO	Chief Executive Officer
MQTT	The Message Queue Telemetry Transport
CoAP	Constrained Application Protocol
D2D	Device-to-device
NAT	Network Address Translation
DTLS	Datagram Transport Layer Security
D2S	Device-to-Service
S2S	Service-to-Service
GDPR	General Data Protection Regulation
D-Dos	Distributed Denial of Service
CIA	Confidentiality, Integrity och Availability
EMP	Elektromagnetiska pulser

1. Introduktion

1.1 Bakgrund

De senaste åren har präglats av en avsevärd tillväxt av Internet och av det ständigt ökade antalet användare. Denna tillväxt följer utvecklingen där Web 1.0 var början och fram till idag med Web 4.0 med intelligenta anslutningar och den snabba utvecklingen av trådlös kommunikationsteknik, inbäddade sensorer, realtidslokalisering och trådlösa sensornätverk (WSN), vilket i sin tur har lett till Internet of Things (IoT). (Guarda, Fernanda, Haz, de la Cruz, Orozco, Alvarez, 2017).

Guarda et al., (2017) beskriver IoT som en fas där människor, processer, data och saker kopplas samman och förvandlar information till handlingar som skapar nya möjligheter och bättre upplevelser. På samma sätt beskriver Abomhara & Køien (2014) IoT, men berättar även att samtidigt som IoT-världen blir större, kommer säkerhetsproblemen att bli fler och fler.

IoT, är ett fenomen som inkluderar mycket eftersom det kan involvera alla saker som är uppkopplade till internet. Rouse (2016) beskriver att ‘Things’, i Internet of Things, kan vara allt ifrån en hjärtmonitor inopererad i en person, ett husdjur med ID-chip till en bil som har inbyggda sensorer för att varna föraren om däcktrycket är för lågt. Följaktligen, IoT är ett konstgjort objekt som kan tilldelas en IP-adress och försedd med förmågan att överföra data över ett nätverk (Rouse, 2016). Med andra ord, IoT handlar om själva anslutningen av enheter till internet. Idag är mycket uppkopplat till internet vilket medför möjligheten att kunna sätta igång kopieringsmaskinen trots att den inte befinner sig i samma rum, åka självkörande bilar eller att industrier använder uppkopplade enheter för en effektivare verksamhet. För de företag som ämnar att förbättra sina processer och datakapacitet, skapar IoT nya och stora möjligheter (Guarda et al., 2017). Följaktligen, IoT gör både vardagen och arbetet både roligare och enklare samtidigt som det ställer krav på säkerhetstänket.

Gollmann (2011) beskriver säkerhet som ett människo-problem som inte kan lösas enbart av ett tekniskt system. Alla användare måste inte vara säkerhetsexperter men de måste samarbeta och följa de regler och rekommendationer som tillhör organisationen men tyvärr är det inte alla som gör det, istället blir de klassade som icke-ansvarsfulla och blir därmed ett av organisationens största hot (Gollmann, 2011). Förutom denna problematik, står organisationer inför en hel del utmaningar gällande IoT.

1.2 Problemformulering

Under julen 2015 kopplades 50 miljoner *nya* enheter upp mot nätverk runt om i världen (Nilsson, 2016). Nilsson (2016) skriver att många uppskattar smarta prylar men enheterna riskerar att bli en motorväg rakt in i nätverket och då en majoritet av användarna av IoT prioriterar teknikens funktionalitet, har det har blivit hög tid att tänka på säkerheten.

Gartner (2017) förutspår att år 2020 kommer 20 miljarder enheter vara uppkopplade till internet och i dessa enheter räknas inte datorer eller smartphones med, utan funktionsfokuserade objekt

som uppkopplade bilar, jetmotorer och kylskåp för att nämna några exempel. Däremot har Statista (2018) redan uppskattat att idag finns det 23.14 miljarder uppkopplade IoT-enheter och att år 2020 förväntas det finnas närmare 31 miljarder IoT-enheter i världen. Eastwood (2017) beskriver att säkerhetsbristen inom IoT är att det ökar antalet portabla enheter bakom nätverkets brandvägg. För tio år sedan behövde vi bara skydda våra datorer, för fem år sedan behövde vi skydda både datorer och smartphones, nu, behöver vi skydda vår bil, hemelektronik och många andra IoT-enheter. Enligt Lee & Lee (2015) saknas så kallade standarder för säkerhet och behandling av integritet för IoT.

År 2020 kommer 65 procent av världens företag införa IoT-enheter i sin verksamhet och mer än 25 procent av de identifierade säkerhetsattackerna i företag kommer involvera IoT även om IoT kommer stå för mindre än 10 procent i företags IT-säkerhets budget (Gartner, 2017). Detta ledde oss till följande forskningsfråga:

Vilka faktorer bör företag överväga gällande säkerhetsbrister i IoT-enheter?

1.3 Syfte

Eftersom informationssäkerhet tillsammans med IoT idag är viktigare än någonsin blir det ämnet högst aktuellt. I en värld där mycket kommer att vara, och är, uppkopplat kommer också säkerhetsrisker att uppstå, både för privat information, företagsinformation och individen i sig. De aktörer som bidrar och bestämmer hur marknaden kan, och ser ut nu, är i många fall företagen. Dessa bär därför på ett ansvar att vara medvetna om säkerhetsrisker vilket vidare kommer diskuteras. Genom en kvalitativ studie med noga utvalda intervjupersoner ska det utredas vilka faktorer företag behöver överväga gällande säkerhetsriskerna som finns vid användandet av IoT-enheter. Studien innehåller intervjuer av aktörer i IT-branschen inklusive företag som använder sig av IoT, som skapar IoT-enheter och experter inom ämnet för att få ett brett perspektiv. Denna studie ämnar till att belysa om vad företag bör beakta för att uppnå en högre medvetenhet gällande säkerhetsbrister i IoT-enheter.

1.4 Avgränsningar

Denna studie är uteslutande inriktad på verksamheter placerade i Sverige och deras kunskap om IoT och säkerhet. Fokus ligger på företag och aktörer i IT-branschen som använder, tillverkar eller har erfarenhet med IoT-enheter och det är dessa typer av företag som kommer att presenteras i studien. Studien begränsas till “saker” (sakernas internet) som är direkt uppkopplade till internet eller en molntjänst, exempelvis övervakningskameror, kylskåp, brödrostar och exkluderar datorer, mobiler och surfplattor. Studien är inte djupgående i den tekniska aspekten av Internet of Things utan kommer att fokusera på säkerhetsaspekter i relation till IoT och informationssäkerhet.

2. Litteraturgenomgång

I detta kapitel presenteras olika teorier, modeller samt ramverk som är relevant för studiens frågeställning och som kommer att vara grundläggande för diskussion och slutsats. För att besvara frågeställningen kommer begreppet IoT och säkerhet förklaras och även sambandet mellan dessa. Även tidigare forskning kommer att redogöras för att både skapa en referensbild av andra verksamheters föreställningar och för att stärka argument och slutsatser.

2.1 Internet of Things

2.1.1 Definition

Definitionen av Internet of Things kan vara svår att precisera, då olika perspektiv ger olika beskrivningar. Enligt Kumar & Patel (2014) är det ett paradigm där saker kan identifiera, känna och processa funktioner som låter enheter kommunicera med andra enheter genom internet. Baserat på en undersökning utfärdad 2015 av Whitmore, Anurag, Li, är det huvudsakliga konceptet av IoT vardagliga objekt som är utrustade med identifierande, kännande, nätverk-och bearbetningsfunktioner som tillåter kommunikation mellan enheter och tjänster via internet för att uppnå ett användbart mål. Medans alla objekt som har en internetuppkoppling kan ses som IoT finns även smalare definitioner tillgängliga exempelvis inom logistik och supply chain management. Där kan IoT referera till objekt med RFID sensorer som tillåter en unik identifikation och övervakning av objektet och köpbeteendet hos kunder (Weber, 2010). Gartner definierar IoT som:

> *"Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment"*
> (Gartner, 2018)

Termen IoT används också som synonym för *ambient intelligence* eller *ubiquitous computing* som refererat till smarta objekt och sensorer samt andra objekt som är medvetna om sitt sammanhang och som kan kommunicera med andra enheter (Dastjerdi & Buyya, 2017). IoT är en förlängning av det internet vi har idag eftersom det integrerar mobila och sociala nätverk tillsammans med "smarta saker" för att ge en bättre service till användaren (Li & Da Xu, 2017). IoT kan alltså referera till ett nätverk av "kännande objekt" som övervakar och registrerar aspekter av deras miljö och användarbeteende (Wachter, 2017). Det huvudsakliga målet med IoT är att göra en bättre värld för oss människor där varje enhet kan förstå situationer och utföra något utan mänsklig förklaring (Kumar & Patel, 2014). Däremot är den exakta definitionen av IoT fortfarande subjektivt beroende på vilket perspektiv man ser på det ifrån (Li & Da Xu, 2017).

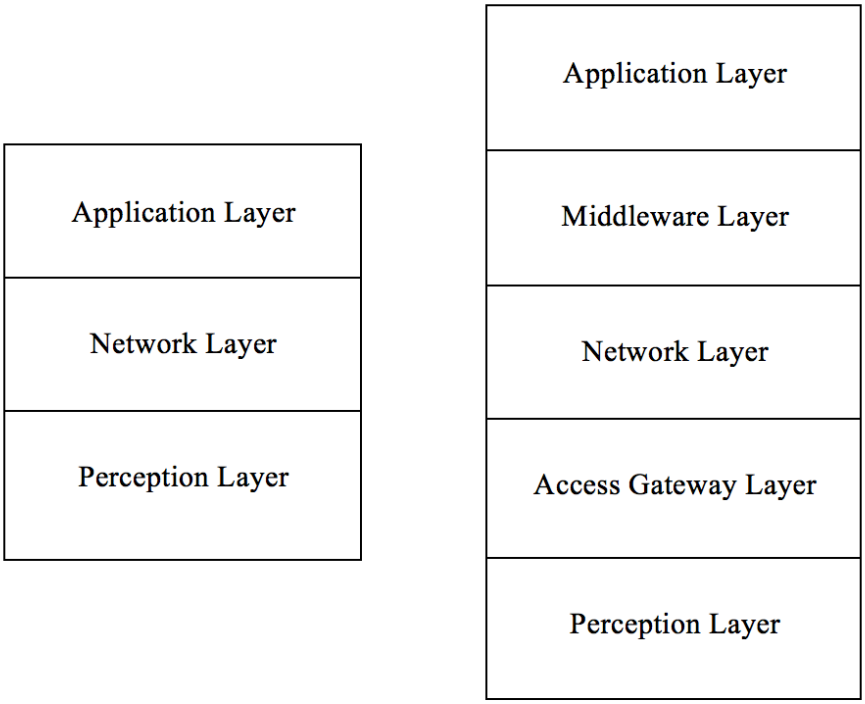
2.1.2 Evolution

Termen IoT hördes först år 1999 när den brittiska teknologen Kevin Ashton beskrev ett system med enheter som var sammankopplade via sensorer (Kumar & Patel, 2014). Termen "Internet of Things" är fortfarande ganska ny men konceptet att använda enheter för att kontrollera och övervaka fanns redan på 1970-talet (Thakare, Patil, Siddiqui, 2016). År 1990 kom den första

uppkopplade brödrosten som kunde stängas av och på via internet och 2001 kom andra saker såsom sodastream-maskiner och kaffemaskiner som var IP-baserade (Thakare et al., 2016). Sedan 2006 har den Europeiska kommissionen arbetat mycket inom IoT och har bland annat diskuterat policy och problem för hur IoT ska styras (Thakare et al., 2016). 2009 presenterade IBM:s CEO konceptet om en "smart planet" där vardagliga saker som flygplatser, elnät, tågtrafik och liknande kommer vara kopplade till sensorer (IBM, 2009). Det är inte bara Europa som satsar på IoT utan även USA och Asien. Till exempel i Sydkorea och Kina har regeringen satsat på avancerad IoT-infrastruktur och forskning (Li & Da Xu, 2017). Utvecklingen har minst sagt gått snabbt fram och den kommer troligen att fortsätta i samma mönster.

2.1.3 Tekniken bakom Internet of Things

För att en organisation ska kunna implementera IoT på ett framgångsrikt sätt krävs det att verksamheten skapar en infrastruktur som kan stödja ett sådant system. Däremot finns det ingen konsensus gällande en IoT-arkitektur som är universellt godkänd som en officiell standard, utan flera olika arkitekturer har visats av olika forskare. Vanligtvis brukar två arkitekturer föredras, antingen en treskiktsarkitektur, vilken kommer beskrivas grundligare, eller en femskiktsarkitektur. (Sethi & Sarangi, 2017)



Figur 1: *Tre- och fem-skiktsarkitektur*

I arkitekturens yttre skikt, **Perception Layer,** finns sensorerna för IoT, som främst används för att identifiera objekt och samla in information. Här inkluderas bland annat kameror, RFID, streckkoder och GPS. Med hjälp av dessa typer av sensorer kan man läsa av vår fysiska omvärld, för att sedan omvandla den till en särskild signal. Denna signal omvandlas därefter till läsbar information som ska kunna tolkas av en människa, eller skicka vidare den via nätverk. (Aazam, Khan, Abdullah Alsaffar, Huh, 2015)

Exempel på sensorer som blir allt mer vanliga i vår vardag är fingeravtrycksläsare, mikrofoner, accelerometrar, avståndssensorer (IoT Sverige, 2017). Enligt IoT Sverige (2017) är användningsområdena för sensorer många, men för att kunna dra nytta av deras resultat krävs det att de placeras på relevanta ställen.

Sethi & Sarangi (2017) beskriver att **Network Layer** ibland kallas för hjärnan av IoT vars huvudfunktion är att bearbeta och överföra information. För att informationen ska kunna överföras från sensor till människa, eller andra enheter, krävs ett nätverk.

Ett nätverk kan beskrivas som en struktur av olika typer av enheter som är sammankopplade och kommunicerar med varandra. Beroende på hur mycket information som man vill skicka mellan enheterna, väljer man en specifik typ av de många olika typer av nätverk. När det kommer till Internet of Things vill man även att enheterna ska kunna kommunicera genom luften, istället för genom kablar, via ett trådlöst nätverk. (IoT Sverige, 2017)

Application Layer använder den behandlade datan från det föregående skiktet, och utgör egentligen hela fronten av arkitekturens struktur. Skiktet kommunicerar direkt med slutanvändaren, och består av olika applikationer med respektive applikationsprotokoll. (Sethi & Sarangi, 2017)

Dessa protokoll används när man ska välja hur man ska gå tillväga när det gäller datakommunikation över nätverk. Protokollen definierar de olika regler och avtal som finns gällande informationsöverföring likt en standard, och innehåller även de tekniker som används (Yassein, Shatnawi, Al-zoubi, 2016). Enligt Jassey (2014), finns det en handfull med protokoll som är att föredra när det kommer till Internet of Things, då man pratar om information som överförs trådlöst till exempel MQTT och CoAP.

Yassein et al., (2016) beskriver att The Message Queue Telemetry Transport (MQTT) fokuserar likt andra protokoll att samla in information från en mängd olika enheter, och därefter överföra den informationen till IT-infrastrukturen. Just MQTT är en typ av device-to-service (D2S) protokoll, som tillåter integreringen av en applikation till en server. Man använder sig av en mellanhand, en så kallad Broker, mellan källan och användaren. Då båda är anslutna till Brokern, men inte med varandra, så är anslutningen inte direkt. Tack vare Brokern behöver källan och användaren inte vara medvetna om varandra sedan tidigare, och behöver inte heller arbeta synkroniserat. Detta sätt av arbete stöds av brandvägg, och störs inte av vad man kallar Network Adress Translation (NAT). MQTT föredras av många IoT-implementerare, då den är enkel att använda. (Novotek, u.å) Däremot har det, enligt Olzak (2017) som skriver om säkerhetsrisker för e-tidningen CSO, nu identifierat att Brokern innebär en säkerhetsrisk, då informationen passerar utan någon typ av autencitering, trafikkryptering eller vanlig kryptering.

Ett annat protokoll som anses varas främst kompatibelt med IoT-system är Constrained Application Protocol (CoAP), som är ett nätverksorienterat protokoll och påminner en hel del om standarden HTTP. CoAP används främst för begränsade enheter och har blivit standardprotokoll för IoT applikationer. (Yassein et al., 2016) För optimal funktionalitet och säkerhet

rekommenderas man enligt Chavan & Nighot (2014) att man ska komplettera CoAP med DTLS, ett slags säkerhetsprotokoll som ser till att kommunikationen mellan enheter är säker.

2.2 CIA Triad

CIA står för *confidentiality*, *integrity* och *availability* och är en modell designad som avser att vägleda policies för informationssäkerhet inom en organisation. De tre elementen anses vara de tre viktigaste komponenterna inom säkerhet. (Rouse, 2014) Definitionerna är inspirerade av Gollmann (2011) och Harris (2002).

Figur 2: *CIA-modellen (Rouse, 2014)*

Confidentiality är den komponent som ser till att information endast är tillgänglig för rätt person samtidigt som man ser till att obehöriga personer inte har tillgång till den. Det är vanligt att information kategoriseras i typ av information, mängd och typ av skador som skulle kunna uppstå om informationen hamnade i obehörigas händer. Uppdelningen görs för att stränga åtgärder ska kunna genomföras. (Rouse, 2014)

För att säkerställa konfidentialiteten av data rekommenderar Agarwal & Agarwal (2011) att företag har nätverkssäkerhetsprotokoll, nätverksautentiseringstjänst och krypteringstjänster. Inom företaget rekommenderas anställda att ha svårgissade inloggningsuppgifter och att gå en säkerhetskurs för att försäkra att de anställda är medvetna om risker och hot som kan påverka dem och företaget, om information läcker ut. (Agarwal & Agarwal, 2011)

Rouse (2014) skriver att komponenten ***Integrity*** innebär att bibehålla noggrannheten och tillförlitligheten av information under hela tiden informationen är riktig. Information får och kan inte inte ändras av obehöriga personer då åtgärder för att kunna upptäcka just detta finns tillgängliga (Rouse, 2014).

Agarwal & Agarwal (2011) beskriver intrångsdetektering, brandväggar och kommunikationssäkerhet som säkerhetsställare för integritet. I vissa fall kan intrångsdetektering vara nödvändigt för att datasäkerheten ska kunna känna av ändringar i data från elektromagnetiska pulser (EMP) för att motstå data- och mjukvarufel (Agarwal & Agarwal, 2011).

Komponenten ***Availability*** innebär, enligt Rouse (2014), att användaren har aktuell och tillförlitlig tillgång till information. För att en användare ska komma åt information måste tre delar fungera och vara sammankopplade nämligen kommunikationskanaler för tillgång, säkerhetskontrollerna som skyddar informationen och datasystemet som lagrar informationen (Agarwal & Agarwal, 2011).

Sammanfattningsvis beskriver Rouse (2014) att confidentiality är en samling regler som begränsar tillgången till informationen, integrity är försäkringen om att informationen är sann och exakt, och slutligen availability är garantin om att informationen är tillgänglig för auktoriserade personer.

2.3 Säkerhet inom IoT

Rouse (2014) nämner att ***IoT privacy*** och ***IoT security*** är några av CIA absolut största utmaningar. *IoT privacy* är de särskilda överväganden som krävs för att skydda informationen från individer från exponering i IoT-miljön, där nästan alla fysiska eller logiska enheter kan ges en unik identifierare och förmågan att kunna kommunicera via internet. Data som överförs av en viss endpoint behöver inte orsaka några privata problem men när data från flera olika ändpunkter samlas och analyseras kan den ge känslig information. (Rouse, 2014)

IoT security är också en utmaning på grund av det stora antalet uppkopplade enheter utöver datorer, som ofta är skyddade med svaga lösenord. Om IoT enheterna inte är tillräckligt skyddade kan de användas som separata angreppsvägar. I en studie visade forskare att ett nätverk skulle kunna äventyras av en Wi-Fi-aktiverad glödlampa vilket tydliggör att säkerhet måste prioriteras lika högt som utvecklingen av internetuppkopplade produkter. (Rouse, 2014)

2.3.1 Säkerhetsbrister

Privacy

"*Rätten att få sin personliga egenart och inre sfär respekterad och inte utsättas för kränkande behandling*" (Art. 8 ECHR).

Privacy handlar om personlig integritet vilket innebär att människor ska kunna förhindra att information om sig själv sprids, med frihet för övervakning och kontroll över personlig information (Hughes, 2015). Enligt Serbua & Rotariua (2015) omfattar personlig integritet saker som tillhör en person såsom hemligheter, känslor, kroppen eller information om sexuell läggning, religion, medicinskt tillstånd och så vidare.

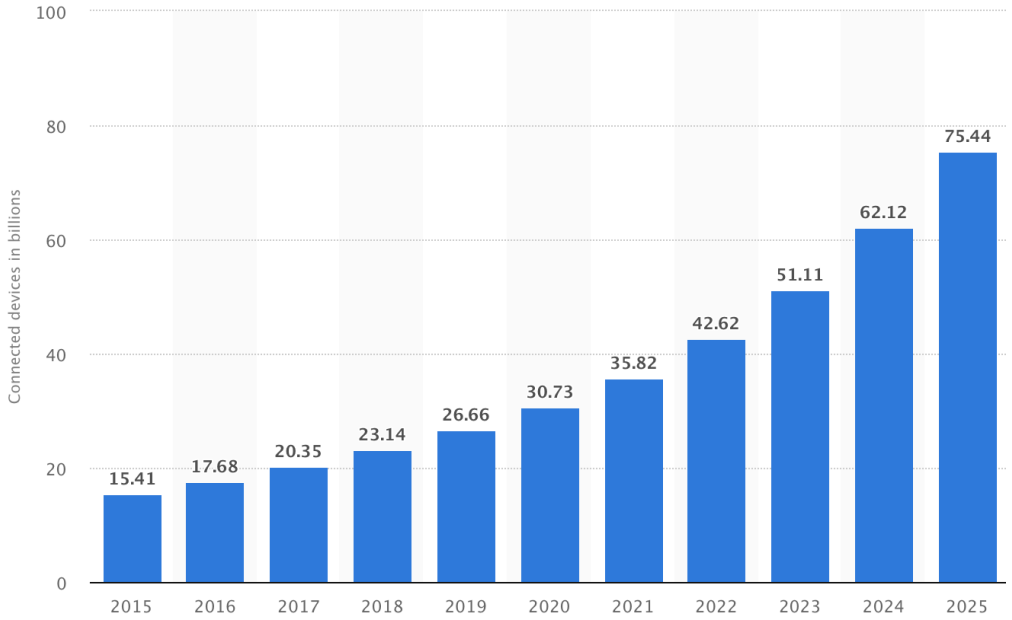
Ett problem som uppstår vid användandet av IoT-enheter är att enheterna samlar så pass mycket information så att det påverkar användares personliga liv då de kan förlora sin personliga integritet. Serbua & Rotariua (2015) menar att information om användare inte längre är privat och enligt Lee & Lee (2015) är lagar om hur man skyddar sin integritet allmänt svaga vilket bidrar till att det sker integritetskränkningar dagligen.

Säkerhetsproblem kommer att kunna lösas genom att träna och utbilda utvecklare att helt enkelt skapa säkra lösningar (Lee & Lee, 2015). Ziegeldorf, Morchon, Wehrle, (2014) skriver att personlig integritet är ett stort hinder för utvecklingen av IoT då användarens uppgifter kan läcka ut om det inte implementeras korrekt.

Mängden enheter

Den största utmaningen med IoT är säkerheten med tanke på den mängd enheter som IoT omfattar vilket ökar och blir då ett påtagligt problem menar Li & Da Xu (2017). Det har ökat från 0,9 miljarder IoT-enheter 2009 till 23,4 miljarder 2018 enligt Statista (2018). Ett exempel är när "smarta städer" förlitar sig på sensorer, RFID och WiFi vilket kan vara offer för cyberattacker och för att ha IoT utspritt i städer krävs att en genomtänkt och säker infrastruktur byggs där systemet visar tydligt om det utsätts för någon säkerhetsrisk (Wachter, 2018). Enligt Kumar & Patel (2014) är inte de traditionella säkerhetsåtgärderna direkt applicerbara på IoT enheter på grund av olika kommunikations *stacks* och nätverksstandarder. Därför måste företag vara vaksamma gällande mängden IoT-enheter och dess säkerhetsåtgärder. Lee & Lee (2015) påstår motsatsen och menar att vid bristande säkerhet och integritet kommer användandet av IoT enheter minskas på både individnivå och i organisationer.

År 2020 förutspås det, som tidigare nämnt, finnas 20 miljarder IoT-enheter enligt Gartner (2017) men enligt Statista (2018) närmare 31 miljarder år 2020. Schaller (1997) skriver att Gordon E. Moore sa, 1995, att tillverkare hade fördubblat tätheten av transaktioner per integrerad krets vid regelbundna intervaller, och de skulle fortsätta att göra det så långt ögat kunde se. Denna observation kommer senare att kallas "Moore's Lag" och är enormt inflytelserik. Moore's lag är alltså inte en fysisk lag, utan det är en mycket pricksäker observation (Holmberg, 2016). Moore's lag säger i grunden att tekniken utvecklas exponentiellt för att bli allt mer kraftfull vilket också är en anledning till att teknisk säkerhet har blivit en större del av vårt liv (Holmberg, 2016). IoT är idag ett bra exempel på hur Moore's lag är en korrekt observation, bara för några år sen var inte IoT lika välutvecklat som det är idag och enheterna blir fler, kraftfullare, mindre och billigare för varje år som går (Witeck, 2016). Statistik från Statista (2018) gällande antal uppkopplade IoT-enheter i världen från 2015 till 2025 visar på just en exponentiell tillväxt (se Figur 3).



Figur 3: *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), Statista (2018).*

Öppen källkod

Enligt Vadalasetty (2003) är öppen källkod bra för att eventuella buggar och brister snabbt kan åtgärdas eftersom fler kan hjälpa till. Däremot kan öppen källkod även vara ett hot just eftersom alla har tillgång till koden, även hackare, så de enkelt kan lista ut hur man ska hacka koden. Precis som Vadalasetty (2003) förklarar, skriver även Mohamed (2008) att gratis öppen källkod är öppen för alla då även hackers vilket kan leda till en säkerhetsbrist eftersom hackarna då vet exakt hur delar av koden ser ut.

Karalov (2018) förklarar att en annan säkerhetsbrist företag har gällande användandet av öppen källkod är att de inte scannar koden för eventuella svagheter. Där är heller ingen dokumentation för hantering av säkerhet gällande öppen källkod och det lämnas dessutom sällan garantier på koden (Karalov, 2018).

Säkerhetsattacker

Den stora mångfalden inom IoT är en sårbarhet som gör att attacker mot tillgängligheten, säkerheten och den personlig integritet kan göra stor skada (Li & Da Xu, 2017). De olika skikten i IoT-arkitekturen har olika sårbarhet och **Network layer** är speciellt utsatt eftersom IoT förlitar sig på nätverk vilket underlättar avlyssning, tillgång till privat information och överbelastningsattacker som Denial of Service (DoS) (Li & Da Xu, 2017). DoS attacker eller Distributed Denial of Service (DDoS) är en attack som är till för att överbelasta ett nätverk, webbplats, datorsystem eller webbtjänst och innebär att all server- eller förbindelsekapacitet kraschar (Sentor, 2018).

Vidare finns det ett annat tydligt problem inom många företag, nämligen att många anställda inte känner sig trygga på sin arbetsplats. Brooks (2015) skriver om ett företag som gjorde en undersökning om hur säkra anställda känner sig på deras arbetsplats gällande fysiska hot från en annan person eller en hacknings attack och kom fram till att 30 procent av cirka 3000 anställda

runt om i USA känner sig osäkra på arbetet. Ännu värre, många vet inte vad de ska göra om en attack sker och 40 procent vet inte om det existerar någon plan för hur en attack ska hanteras om det händer företaget (Brooks, 2015). Post (2016) skriver om vikten av att förbereda ett företag och de anställda för en potentiell katastrof och menar att om företaget har framställt en plan för att hantera attacker skapas automatiskt en trygghet och tillit från de anställda till företaget. Även om det sker en attack kommer skadan bli betydligt mindre om en plan för hur det ska hanteras finns (Post, 2016).

Enligt Accenture Security (2018) har organisationers återhämtningsförmåga inom datasamhället förbättrats trots ett ökat tryck från inriktade säkerhetsattacker, som har fördubblat sedan 2017. Enbart en av åtta attacker lyckas under 2018, om man jämför med en av tre attacker för bara ett år sedan. I en undersökning svarar 83 procent att man tror att nya genombrottstekniker som till exempel Artificiell Intelligens, machine learning, analyser av användarbeteende samt blockchain är väsentliga för att säkerhetsställa framtiden för deras organisation. Genom ett växande stöd och ökade investeringar i IT-säkerhet de senaste åren börjar nu företagsledningar få en större medvetenhet gällande säkerhetsattacker. (Accenture Security, 2018)

2.4 Teoretiskt ramverk

Nedan introduceras det teoretiska ramverk som sammanfattar nyckelkoncepten som identifierats i litteraturgenomgången. Tabell 1 (se nedan) belyser koncepten först genom att beskriva kategori, därefter presenteras studierna som speciellt beskriver den kategorin och sen beskrivs vad de studierna undersöker som är en viktig roll för designen och utformningen av den empiriska studien.

Tabell 1: *Teoretiskt ramverk*

Kategori	Litteratur	Undersöker
Internet of Things	Kumar & Patel (2014) Whitmore et al. (2015) Weber (2010) Gartner (2018) Khodadadi et al. (2017) Li & Da Xu (2017) Wachter (2017) Thakare et al. (2016) IBM (2009)	- Definition - Evolution - Historia
Tekniken bakom IoT	Sethi & Sarangi (2017) Aazam et al (2015) IoT Sverige (2017) Yassein et al (2016) Jassey (2014) Novotek (u.å)	- Infrastruktur - Tre-skiktsarkitektur - Fem-skiktsarkitektur - Application Layer - Middleware Layer - Network Layer

	Olzak (2017) Chavan & Nighot (2014)	- Access Gateway Layer - Perception Layer
CIA triad	Rouse (2014) Gollmann (2011) Harris (2002) Agarwal & Agarwal (2011)	- Confidentiality - Integrity - Availability
Säkerhet inom IoT	Rouse (2014) Art. 8 ECHR Hughes (2015) Serbua och Rotariua (2015) Lee & Lee (2015) Ziegeldorf et al. (2014) Li & Da Xu (2017) Statista (2018) Wachter (2018) Kumar & Patel (2014) Schaller (1997) Holmberg (2016) Witeck (2016) Vadalasetty (2003) Mohamed (2008) Karalov (2018) Sentor (2018) Bisson (2018) Brooks (2015) Post (2016) Accenture Security(2018)	- Säkerhetsbrister - IoT security - IoT privacy - Personlig integritet - Mängden enheter - Moore's lag - Öppen källkod - Säkerhetsattacker - DDoS

3. Metod

I detta kapitel förklaras den metod som står till grund för hur studien är utförd i syfte att besvara forskningsfrågan. Det beskrivs vad för teori som behandlats och varför samt metodval för insamlingen av den empiriska datan och hur urvalsprocessen sett ut. Vidare beskrivs intervjustruktur och processen kring analyserandet av den empiriska datan samt tillvägagångssätt. För att säkerställa att undersökningen höll hög kvalite innehåller metoden aspekter som beaktas i utformningen av studien.

3.1 Val av teori

Litteraturen är baserad på artiklar, böcker och studier som är högst relevanta för undersökningen då den behandlar samma område som undersöks och är skrivna i nutid vilket är viktigt då det är ett ämne som växer otroligt snabbt. Huvudsakligen har vi använt oss utav Google Scholar men även använt litteratur från olika bibliotek på Lunds Universitet för att finna relevant information relaterat till säkerhet, IoT och medvetenhet. Sökningarna har främst genomförts på engelska just på grund av att de flesta studier om säkerhet och IoT är skrivna på engelska. Sökord som använts inkluderar IoT, IoT environment, IoT security, data security, security awareness med flera. Dessa sökord har givit oss intressant information som sedan har använts som teori.

Den teoretiska undersökningen har lett till att vi lyckats identifiera koncepten relaterat till infrastrukturen av Internet of Things. Efter påbörjad undersökning om evolutionen av IoT identifierades olika skikt som IoT är uppbyggt på, nämligen Application Layer, Network Layer och Perception Layer. Liknande identifierades CIA-triaden som består av Confidentiality-, Integrity- och Availability-komponenterna. Vidare gällande det teoretiska ramverket, har dessa aspekter varit högst viktiga för utformningen av intervjuguiden. Trots att aspekterna kan ha en tekniskt drivande väg tar vår intervjuguide respondenterna från den synvinkeln, för att få in den strategiska kunskapen om hur de klarar av den snabba utvecklingen av teknik som IoT och de ständigt utvecklande säkerhetsfrågorna, adresserad i termer av CIA.

I denna studie är det teoretiska ramverket baserat på ett flertal teoretiska koncept som huvudsakligen behandlar IoT, IoT-infrastruktur, beståndsdelarna gällande informationssäkerhet som är beskrivna i CIA, samt även generella säkerhetsaspekter inom IoT. Det teoretiska ramverket spelar en viktig roll för att hjälpa oss att bättre förstå varför frågeställningen är relevant. Vidare har vi även läst övriga teoretiska koncept, exempelvis privacy-relaterade studier och cloud computing. Till exempel, många privacy-relaterade koncept fokuserar på studier som undersöker personlig integritet på sociala medier där delning av information är huvudpunkten (John, 2012) och cloud computing behandlade teknologier (Botta, de Donato, Persico, Pescapé, 2016) som presenterade motsatsen till IoT. Trots att sådana studier är intressanta och behöver uppföljning för att hantera IoT-evolutionen, har vi inte behållt dem i vår litteraturgenomgång och därmed inte i det teoretiska ramverket, eftersom vi anser att de ligger utanför vår studie.

CIA-modellen valdes eftersom vi ansåg att det gav en tydlig grund för hur informationssäkerhet ska behandlas. CIA-modellen täcker de viktiga delarna för ett lyckat säkerhetsarbete och sambandet mellan dem.

3.2 Insamling av empirisk data

3.2.1 Datainsamling

Jacobsen (2002) kallar den strategi för att samla in data, likt vår datainsamling, för deduktiv datainsamling. Deduktiv datainsamling innebär att man först skaffar sig förväntningar om hur världen ser ut och därefter gå ut och samla empiri för att se om förväntningarna stämmer överens med verkligheten. Kritiken mot denna strategi är att den oundvikligen leder till att forskaren enbart letar efter relevant information och som därmed ger stöd åt förväntningarna som redan är bestämt. (Jacobsen, 2002)

Enligt Jacobsen (2002) är en kvalitativ metod för datainsamling mest lämplig när undersökarna inte vet mycket om undersökningsämnet och när urvalet av intervjuer inte är slumpmässiga. Jacobsen (2002) beskriver också att kvalitativa data är data som presenteras i mening till skillnad från kvantitativ data som oftast presenteras med siffror. Detta medförde till vårt val blev just en kvalitativ undersökning, på grund av dess simplicitet och effektivitet. Utöver det har vi valt att utföra en intensiv undersökning vilket innebär att vi inte kan göra någon generalisering om vad omvärlden säger utan enbart referera till enstaka uppgifter.

3.2.2 Urval

Urvalsprocessen riktade sig till personer i IT-branschen som har kunskap inom IoT och säkerhet för att samla in så kvalitativ data som möjligt. De företag som kontaktades var företag som tillverkar IoT, använder sig av IoT, har kunder som använder IoT och experter som forskar inom området. Personerna som intervjuades har olika erfarenheter inom IoT och kommer från olika typer av företag, tillverkande företag, konsultföretag och ett forskningsprojekt. Gemensamt för respondenterna var att alla har kunskap och arbetar på något sätt med IoT och säkerhet. För att få ett varierat perspektiv samt åsikter för att kunna täcka säkerhetsproblemen inom IoT, valdes dessa varierade respondenter.

Kontakten inleddes med e-postkonversation med samtliga företag, med försprång på u-blox som vid tillfällen är arbetsplats för en av oss författare. Intervjuförfrågan påbörjades med en presentation om oss, syftet med vår uppsats samt dess relation IoT och säkerhet, följt av förfrågan om intervju med lämplig person på företaget. Detta ledde till totalt fyra intervjuer varav tre var på företag och en på Lunds Tekniska Högskola. Atea blev första intervjun för att de har stor kundrelation med IoT i fokus. u-blox intervjuades med anledning till att deras fokus ligger på att designa IoT-enheter eller små moduler som ska placeras i produkter så att de kan bli IoT enheter. Tredje aktören som kontaktades var Martin Hell, docent i informationsteori och lektor i datasäkerhet på LTH och arbetar med projektet Seconds som arbetar och forskar inom säkerhet för uppkopplade produkter och IoT.

Tabell 2: *Sammanställning av samtliga intervjupersoner*

Företag	Namn	Typ av intervju	Position	Tid	Dokumentation
Atea	Mikko Verlinna och Christer Böke	Semistrukturerad, gruppintervju	Verksamhetsutvecklare och Säljspecialist	60 min	Anteckningar
u-blox 1	Mats Andersson	Semistrukturerad, individuell intervju	Senior Director Technology	60 min	Inspelning + anteckningar
u-blox 2	Martin Jerling	Open ended, individuell intervju	Senior Engineer	23 min	Inspelning
LTH, Seconds	Martin Hell	Semistrukturerad, individuell intervju	Docent i informationsteori och lektor i datasäkerhet, LTH. Projektledare, Seconds.	36 min	Inspelning

3.2.3 Intervjustruktur och metod

Jacobsen (2002) förklarar att kvalitativa studier kan genomföras med hjälp av semistrukturerade intervjuer där frågorna är bestämda på förhand, men som ger undersökaren möjlighet att ställa följdfrågor när ett mer omfattande eller förklarande svar behövs. Metoden ger även intervjuobjektet möjligheten att svara med utförliga och breda svar (Jacobsen, 2002). En semistrukturerad intervju innebär att man tidigare har utformat en intervjumall där förutbestämda frågor finns listade, baserat på teori (Jacobsen, 2002). Intervjumallen vi använde oss av hade tre delar, en del för företag som använder sig av IoT produkter och en del om de tillverkade IoT samt en för forskning inom IoT. Detta för att vara förberedd beroende på vad företaget arbetade med. Inför intervjun med Martin Hell gjordes en ny intervjumall som fokuserade på forskningsaspekten samt generellt hans uppfattning om IoT, säkerhet och medvetenhet.

En semistruktur ger, enligt Jacobsen (2002), möjligheten att ställa följdfrågor för att få ytterligare detaljerade svar samtidigt som samtliga intervjuer följer samma röda tråd. Med andra ord, samtliga respondenter kommer att få svara på samma grundfrågor men beroende på deras svar utformar vi egna frågor för att få fram så mycket information som vi kan. Därför tillkom spontana frågor i varje intervju som bidrar till mer kvalitativt resultat.

Vår intervjustruktur under alla förutom en av våra intervjuer är av semistrukturerad karaktär. Den som inte var av semistrukturerad karaktär var en spontan intervju och blev av karaktären öppen intervju. En öppen intervju innebär enligt Jacobsen (2002) att respondenten samtalar som i en vanlig dialog och även den lämpar sig när få enheter undersöks. Vi använde oss utav några av intervjufrågorna under denna intervjun men inte alla utan vi lät respondenten berätta fritt om sin erfarenhet gällande IoT och säkerhet.

Intervjun startade alltid med att vi presenterade oss, frågade om inspelning var okej och därefter fick intervjupersonen presentera sig följt av att vi frågade de frågor som de sedan besvarade. Intervjufrågorna behandlar ämnen som är direkt eller indirekt relaterade till säkerhet, IoT och medvetenhet. Genom att begränsa frågorna ökar chanserna att svaren vi får är av hög relevans och att de går att jämföra med teorin och om vi ställer frågor som "hur hanteras kraven?" får vi, enligt Kvale (1996), spontana, ärliga och fylliga svar från objektets egna erfarenheter.

Jacobsen (2002) menar att det inte är en bra idé att endast föra anteckningar, då det ofta leder till att intervjun inte flyter lika bra som när man inte antecknar. Detta för att för om ett samtal ska flyta på ordentligt krävs ögonkontakt (Jacobsen, 2002). Vi valde således att spela in intervjuerna på våra telefoner. På vår första intervju stannade inspelningen efter cirka tio minuter utan att vi märkte det vilket senare resulterade i att vi snabbt fick skriva ner allt som vi kom ihåg från intervjun. Under följande intervjuer hade vi alltid två telefoner som spelade in intervjuerna för att minimera risken att samma sak skulle hända igen.

Direkt efter varje intervju gjorde vi en transkribering för att så mycket information som möjligt skulle ligga färskt i minnet. Intervjuer skrivs oftast ut ordagrant inklusive pauser och andra ljud (Olsson & Sörensen, 2011). Intervjuerna har således transkriberats ordagrant, inklusive talspråkliga uttryck likt "eh", "aa" med flera. Detta för att ge ett så bra resultat av intervjuerna som möjligt. Alla anteckningar och transkriberingar som gjorts har vi mailat till respektive företag som sedan har godkänt dem, detta har vi gjort för att säkerställa att vi uppfattat informationen de givit oss korrekt.

3.2.4 Intervjuguide

Nedan följer den intervjuguide som utvecklades inför intervjuerna för uppsatsens empiri. De semistrukturerade frågorna skickades i nästan alla fall ut till intervjuobjekten innan intervjun för att förbereda och låta intervjuobjekten reflektera och svara på bästa möjliga sätt (Jacobsen, 2002). Intervjuguiden är uppdelade i tre delar eftersom intervjuobjekten arbetar och har erfarenhet av IoT och säkerhet från tre olika perspektiv. Delarna behandlar framförallt *confidentiality*, *integrity* och *availability*, samt de olika skikten i IoT-arkitekturen. Till vissa intervjuobjekt ställdes frågor från fler än en del för att få ut så mycket som möjligt från intervjun. När det ställdes spontana frågor var det oftast kopplade till de ämnen vi ville ta upp och från litteraturgenomgången.

Vilka faktorer bör företag överväga gällande säkerhetsbrister i IoT-enheter?

Vi har valt att fokusera på uppkopplade* IoT-enheter, inte datorer, surfplattor och mobiler utan kopieringsmaskiner, övervakningskameror, larmsystem och så vidare. Vi har upptäckt att säkerheten inte prioriteras i dessa produkter och vill utforska det ytterligare. Vi vill också utreda hur pass medvetna företag är om de risker som finns med uppkopplade enheter.

* Med uppkopplade produkter menar vi saker som är uppkopplade till internet. Produkter som skickar information till ett moln utan komplexiteten som en dator, surfplatta eller mobil har.

Inledande frågor

- Är det okej om vi spelar in?
- Vi presenterar oss och berättar om kandidatuppsatsen
- Intervjupersonen berättar om sig själv och sin yrkestitel
- Berätta lite om företaget/projektet?

Bakgrundstankar

- Medvetenhet
- Bild av säkerhet och säkerhetsbrister
- Konsekvenser
- Åtgärder

Del 1 - *Om intervjuobjektet har IoT-produkter i sin verksamhet*

- Anser ni att uppkopplade enheter är ett problem, dvs att de utgör en risk för potentiellt dataintrång eller för organisationen överlag? Varför?
- Vad för slags enheter har ni vardagligen uppkopplade till internetet?
- Vad gör ni för att säkerhetsställa att er information är säkert lagrat?
- Är du medveten om riskerna som finns med uppkopplade enheter?
- Hur arbetar ni med medvetenheten av säkerhetsrisker hos anställda i ert företag?
- Arbetar ni proaktivt med hantering av säkerhetsrisker? I så fall hur?

Del 2 - *Om intervjuobjektet arbetar i en verksamhet som tillverkar IoT produkter*

- Tillverkar ni uppkopplade produkter?
- Vilka krav ställer era kunder på säkerheten på era produkter?
- Är kunderna medvetna om att det kan finnas säkerhetsrisker?
- I vilken ordning prioriterar ni att era produkter är tillräckligt säkra?
- Vad gör ni som utvecklare av IoT-produkter för att se till att era kunder är medvetna om de risker som de kan potentiellt kan behöva bemöta?

Del 3 - *Om intervjuobjektet forskar inom IoT*

- Vad är din yrkestitel?
- Hur kommer det sig att du valt att fokusera på just den inriktningen (om den är IoT)?
- Du har jobbat med ditt projekt "Seconds". Vill du berätta lite om det?
- Säkerhet, skulle du säga att det är en "trend"? Varför blev den viktig bara för två år sedan? Personlig åsikt gällande säkerhetsbristen?
- Vad tror du är den underliggande anledningen till varför man inte prioriterat säkerheten?
- Hur tror du att framtiden kommer att se ut?

Teknik

- Vi har en bild hur ett IoT-system är uppbyggt med antingen en tre- eller femskikts arkitektur, som vi har förstått det som. Hur ser din bild av tekniken kring Internet of Things ut?

Figur 4: *Intervjuguide*

3.2.5 Geografisk plats

Enligt Jacobsen (2002) är det fördelaktigt om intervjuer sker i en naturlig miljö för intervjuobjektet, exempelvis på deras kontor, eftersom människors beteende lätt påverkas av omgivningen. På grund av detta, valde vi att genomföra samtliga intervjuer på intervjuobjektets kontor för att minimera påverkan så mycket som möjligt samt genom videokonferens. Samtidigt som intervjuobjektet är i en naturlig och bekväm miljö kan förstås problem uppstå. Att utföra intervjuer på intervjuobjektets kontor kan innebära störande moment såsom kollegor, telefonsamtal och så vidare (Jacobsen, 2002). Under en av våra intervjuer hände just detta, men vi anser dock att det inte påverkade själva intervjun mer än att det blev en kort paus. Vi anser också att utföra intervjuer på intervjuobjektets kontor innebär att de inte behöver lägga tid på att förflytta sig till en annan plats och har då större möjlighet att hinna med en intervju. En annan fördel med att ha intervjuer på respondentens naturliga miljö är att man träffar på fler människor vilket vi gjorde. Medans vi gick en rundvandring på företaget stötte vi på en kollega till respondenten som frågade vad vi skrev om och tyckte direkt att vi skulle prata med honom. Vi fick alltså en spontan intervju på plats, vilket gjorde intervjun lite ostrukturerad men också mycket givande och avslappnad.

Vi utförde även en gruppintervju via Skype med video vilket är likvärt en intervju i verkligheten. En gruppintervju är högst lämplig vid kvalitativa undersökningar enligt Jacobsen (2002) vilket var ett skäl till varför vi provade den metoden också. Jacobsen (2002) beskriver dock telefonintervjuer som ett problem då samtalen ofta begränsas. Skype-intervjun, i vårt fall, var ett mycket öppet och givande samtal som inte kändes begränsad över huvud taget.

3.2.6 Etik

Jacobsen (2002) förklarar vikten av de etiska aspekterna i en undersökning. Han menar att det är av yttersta vikt att intervjuobjekten deltar frivilligt i undersökningen, samt att de fått tillräckligt med information för att ta beslutet att delta eller inte. Jacobsen (2002) förklarar även att det bästa tillvägagångssättet inte är att ge intervjuobjekten full information om vad som ska undersökas eftersom intervjuobjektet då kan påverkas och omedvetet lämna information som är anpassad till undersökningen. Detta kan i sin tur leda till felaktiga data (Jacobsen, 2002). Jacobsen (2002) beskriver även vikten av att respektera respondenternas rätt till privatliv, att privata frågor ska undvikas, att hänsyn bör tas till känslig information samt att försiktighet bör iakttas gentemot frågor vars svar kan identifiera anonyma personer.

Eftersom vi visste att det är viktigt att låta respondenterna delta frivilligt och att låta de avstå från frågor om de inte kände sig bekväma med att svara på dem, uttryckte vi det redan under vår mailkontakt. Exempelvis tog de upp att särskilda frågor gällande sekretessdetaljer helst skulle undvikas. Detta, upplevde vi, bidrog till en bättre tillit mellan oss och respondenterna vilket också kan ha gett oss mer information än om vi inte uttryckt oss om det.

4. Empiriska resultat

I denna del kommer det analyserade empiriska material som samlats in under intervjuer att redovisas. Respondenternas svar har behandlats utifrån deras åsikter och erfarenhet gällande IoT, säkerhet och medvetenhet.

4.1 Respondenterna

Respondent 1 och 2 Atea

Atea är marknadsledande inom IT-infrastruktur i Norra Europa och de Baltiska länderna med sina 6900 anställda. Respondenterna från Atea bestod av en säljspecialist inom säkerhet, Christer Böke, och en verksamhetsutvecklare med fokus på säkerhet, Mikko Verlinna. Att respondenterna jobbade på två olika kontor i Sverige, Eskilstuna och Malmö, samt de olika arbetsuppgifterna gav olika perspektiv på Ateas verksamhet och en varierad intervju. Respondenterna förklarade att de åsikter och tankar som framstod på intervjun var deras egna och inte nödvändigtvis Ateas, därför visar denna empirin perspektivet på säkerhet och IoT från den anställdas och dess egna erfarenhet från arbetslivet. Respondenterna förklarade att Atea hade mycket få uppkopplade enheter inom sin verksamhet och det var printers, TV-skärmar och liknande. Däremot använder många av Ateas kunder uppkopplade IoT enheter inom sin verksamhet samt använder Ateas tjänster gällande print och kopieringsmaskiner uppkopplade till internet. Här användes en intervjumall riktat till företag som använder sig av uppkopplade produkter men många spontana följdfrågor ställdes gällde deras kunder och deras relation till IoT och säkerhet.

Respondent 3 u-blox

Vi fick kontakt med Mats Andersson, som arbetar som Senior Director Technology på u-blox genom tidigare kontakter. u-blox verksamhet ligger inom ramen för utveckling av trådlösa moduler för användar-, självgående och industriella marknader. Vi visade snabbt ett intresse för företaget då mycket av deras utvecklingen fokuserar på just Internet of Things, och framförallt säkerheten som de försöker implementera i ett tidigt stadie i sina produkter. Mats beskrev med ett tydligt engagemang om både hans personliga och yrkesmässiga intresse i den framgångsrika utvecklingen av IoT. I intervjun förklarades det även att u-blox som verksamhet inte själva använder sig av IoT-enheter, i alla fall inte ännu, men att man lägger stor vikt kring att deras produkter ska vara så säkra och användarvänliga som möjligt för deras kunder. u-blox arbetar enligt principen att alltid försöka ligga steget före vilket är en av anledningarna till att man valt att inte bara prioritera funktionerna, utan även säkerheten. Man har de senaste åren uppmärksammat en växande trend bland många företag som har tagit åt sig rekommendationerna gällande säkerhetsåtaganden, och då har man på u-blox bland annat valt att redan i sina moduler, som företagen då köper och använder i sina huvudsakliga produkter, förse dem med de kravspecifikationerna som behövs.

Respondent 4 u-blox

Den andra respondenten på u-blox, Martin Jerling, är Senior Engineer och fokuserar mycket på säkerhet gällande infrastruktur och produktreleaser. Martin, till skillnad från Mats, arbetar mer med att se till att krypteringsnycklarna på deras produkter är korrekta och att de gått igenom

säkerhetskontroller, samt att de är säkert förvarade. Martin är således mer tekniskt inriktad och arbetar framförallt med mjukvara. Han har mer erfarenhet gällande tekniska aspekten av säkerhetsarbetet gällande säkerhetsattacker, kryptering, hårdvara och mjukvara.

Respondent 5 LTH

I en artikel, skriven av Anders Thoresson (2017), som vi läste relaterat till vår uppsats blev Martin Hell intervjuad och berättar hur han som projektledare driver ett projekt med fokus på att försöka hjälpa företag att upptäcka säkerhetshål i IoT-enheter. Projekt som kallas för Seconds arbetar han, tillsammans med studenter och företag, med att få fram ett verktyg för att göra det enkelt för företag att upptäcka säkerhetshål i IoT-enheter. Martin är således mycket kunnig i ämnet IoT men han är även docent i informationsteori och lektor i datasäkerhet på LTH. Det var så vi blev intresserade av att intervjua honom. Under intervjun berättade han om sin syn på IoT och säkerhet från sin erfarenhet både som projektledare i Seconds men även från ett forskningsperspektiv. Han har mycket kunskap om företags medvetenhet och arbetssätt gällande ämnet då många It-företag ingår i projektet Seconds, exempelvis Axis, Sony och Ericsson.

4.2 Resultat av empiri

4.2.1 Medvetenhet

Företagskunder

När det gäller om kunder är medvetna om säkerhetsrisker gällande uppkopplade IoT-enheter förklarade respondent 1, 2 och 3 att förvånansvärt många av deras kunder inte är medvetna om detta och att säkerhet i många fall inte prioriteras. Respondent 3 och 5 menar på att många kunder tidigare prioriterat funktionalitet framför säkerhet, då det är funktionalitet som säljer. Precis som företagskunder gör respondent 5 en jämförelse med privatpersoner och tar upp ett bra exempel när man ska välja mobiltelefon “Om ni ska jämföra två mobiltelefoner, Samsung och iPhone. Vad jämför ni då? Jämför ni säkerheten eller är det något annat ni jämför?” Här är verkligen ett tydligt exempel på att säkerheten kommer i andra hand hos kunder vilket också gör att vissa företag inte prioriterar det särskilt högt.

Vidare förklaras det att u-blox:s kunder vet att säkerhet är viktigt men kan ha svårt att definiera vad de behöver eftersom säkerhet är så pass brett område så därför följer kunderna oftast sin bransch olika krav, säger respondent 4.

Däremot har medveten ökat i takt med mängden attacker, påpekar respondent 3 och 5 och menar att tack vare expansionen av IoT har även nya sätt att attackera ökat, och att företag idag på grund av det väljer att prioritera säkerhet mer och mer. Framför allt menar man på att säkerhet inte var lika ‘upptäckt’ för två år sen, som det är idag. I alla fall inte av majoriteten av företagen, påstår respondent 3.

Även om Ateas kunder sällan har något krav på säkerhet brukar inte respondent 1 och 2 ha för vana att “sälja på” sina kunder säkerhetslösningar. Säkerhetslösningar säljs bara om kunden

ställer krav på detta och därmed ber om det. Däremot brukar kunder vilja ha "hela paketet" från Atea där säkerhet ofta ingår. De tar upp ett exempel på när kunder inte är medvetna om säkerhetsfunktioner nämligen när det gäller printers. Själva print-företaget kan ha många säkerhetsfunktioner inbyggt i enheten men användaren aktiverar i många fall inte dessa på grund av lågt säkerhetstänk eller okunskap helt enkelt.

u-blox:s kunder ofta är företag som använder deras moduler i sina egna produkter som i sin tur säljer vidare till deras kunder. Respondent 4 berättar att de kan få specifika krav på en produkts säkerhet från en kund men oftast har vill de bara uppnå en specifik standard som deras egna kunder kräver. Enligt respondent 4 har u-blox en löpande diskussion med varje kund för att öka medvetenheten om de risker som finns gällande säkerheten. Ibland har kunden en säkerhetsexpert med sig eller branschstandarder som ska uppfyllas.

Som tillverkande företag har u-blox ett ansvar gentemot sina företagskunder att integrera säkerhet i sina produkter eller informera om de hot som finns mot respektive modul. Respondent 4 berättar att u-blox förklarar säkerhetsbristerna för sina kunder men att det kan vara svårt att ge garantier och menar att de arbetar fortlöpande med säkerheten med kunderna. Han berättar även att han tycker att de måste bygga in i deras arkitektur så att de kan ha uppdateringar för att kunna spåra vad och var det går fel. På så sätt kommer de kunna ha övervakning över marknaden. Vidare beskriver han att de kommer senare att kunna garantera att de följer best practises eller att de uppfyller någon certifiering.

Företag i allmänhet

Empirin visar att det kan bero på två faktorer gällande vissa företag som generellt är mer medvetna om säkerhetsrisker inom IoT. För det första gäller det storleken på företaget. Respondent 1 och 2 upplever att större företag generellt är mer medvetna om säkerhetsrisken med IoT. Detta upplevde även respondent 4 som berättar att större kunder har större möjligheter och bättre koll och att de har oftast personer som är specifikt utsatta för säkerheten. Respondent 3 och 5 påstår liknande, att större företag har större chans att vara medvetna då man ofta ha både en tillsatt grupp inom organisation som tar hand om just säkerhetsdelen, samt att man har resurserna. Däremot vet man att det ofta inte prioriteras ändå. Allmänt visar empirin att större företag är mer medvetna om hur viktigt säkerhet är eftersom det finns ekonomi och resurser för att faktiskt kunna prioritera säkerheten. Den andra faktorn är vilken inriktning företaget har vilket respondenterna 1, 2 och 3 håller med om samt det kan vara därför de är medvetna om säkerhetsproblem. Respondent 1 och 2 tog upp exempel som advokatbyråer eller sjukhus, ställen där informationen verkligen måste hållas säker och där säkerhetstänket redan är implementerad i verksamheten.

När det gäller att använda uppkopplade produkter på arbetsplatsen är det olika mellan respondenterna. u-blox har inte några IoT enheter förutom de moduler som de själva tillverkar. Om de skulle ha IoT-enheter på arbetsplatsen skulle de göra säkerhetsanalyser på vad som är skyddsvärt och "threat modelling" för att titta på vilka attack ytor som finns och försöka minimera dem, förklarar respondent 4.

Offentlig sektor

Enligt respondent 5 försöker myndigheter att driva den stora säkerhetsfrågan om att bygga system som är svåra för obehöriga att ta sig in i och eftersom de har makten att sätta lagar och standarder är det otroligt viktigt att de lyfter just den frågan. Respondent 5 menar även på att det inte finns tillräckligt med straff för de som inte följer reglerna vilket i sin tur bidrar till att folk inte riktigt tar det på allvar.

Respondent 1 och 2 tog upp ett exempel om en utbildning vid Mälardalens högskola, Master's programme in Intelligent Embedded Systems. Utbildningen innehåller att elever ska lära sig att skapa uppkopplade produkter genom utveckling och design men till förvåningen ingår där inte någon säkerhetskurs. Respondenterna anser att detta är ett mycket stort problem. Studenterna lär sig att skapa och designa dessa enheter men får inte chansen till att lära sig det säkerhetstänk som krävs idag och blir då felprioriterat redan från start. Däremot säger respondent 5 att fler och fler på Lunds Tekniska Högskola väljer att inrikta sig på just säkerhet och menar att kompetensen förmodligen kommer att växa.

4.2.2 Säkerhetsbrister inom IoT

Något som respondent 1 och 2 belyste gällande dataintrång var att förr och även nu är datorer, surfplattor och mobiler i fokus och säkerhetslösningar för dessa så som brandväggar och liknande prioriteras i första hand. En problematik de belyste var när anställda ta med sig datorer och liknande hem och kopplar upp till sitt privata ADSL modem/WiFi. Om det inte finns något krypteringsskydd eller liknande kan den anställdes privata IoT produkt eller produkter hemifrån utgöra en risk för hela organisationen om organisationen inte har rätt skydd.

Respondent 4 förklarar att en stor utmaning är att veta var den svagaste länken i säkerheten är och att hela tiden försvara sig mot hot man inte vet om. Respondent 3 påstår liknande och menar att man hela tiden måste ligga ett steg före. Samtidigt så beskriver respondent 5 att när ny teknik utvecklas så utvecklas ny kod och då kommer det att finnas hål i den koden också.

Respondent 1 och 2 berättade om självstyrande fordon och om problemet att säkerhetstänket ligger mer på själva säkerheten gällande hur väl den håller sig på vägen och hur bra den upptäcker fordon som är nära. De menar då på att säkerhetstänket finns där men bara hälften, de fokuserar inte på informationssäkerheten, till exempel att bilens mjukvara kan hackas. En annan säkerhetsbrist som respondent 5 beskriver är bristen på utvecklare. Respondent 5 förklarar att många företag som inte har tillräckligt hög kompetens gällande säkerhet vill ta in den kompetensen men stoppas då det är brist. Enligt en studie saknades 750 000 utvecklare i EU för tillfälligt vilket är otroligt oroväckande.

Mängd enheter

Respondent 4 förklarar att fler hot tillkommer i och med att deras moduler går ut i miljontals exemplar och om dessa enheter blir kapade kan de ställa till med väldigt stor skada på internet eftersom de kan skicka stor mängd trafik. Respondent 3 berättar att idag uppskattas mängden enheter till ungefär åtta miljarder enheter, men att man inom bara några år kommer kunna uppskatta mängden till 100 miljarder.

När det gäller mängden uppkopplade enheter berättar respondent 4 att man kan ta bort nätverk för att använda DDoS attacker om man vill slå ut internet vilket gör själva end-noden det intressanta. Därför är själva mängden enheter intressanta och inte vilken data enheten kan hålla. Om man knäcker en nyckel i en typ av IoT-enhet kan man kontrollera alla av samma typ vilken kan användas till överbelastningsattacker berättar respondent 4.

Privacy

Respondent 1 och 2 beskriver att inom säkerhet är identitetshantering vanligt och liknar detta vid nycklar till olika rum. Alla behöver inte ha tillgång till alla rum och behöver därför inte alla nycklar. För att behålla sin personliga information är identitetshantering viktigt enligt dem. Med liknande påstående säger respondent 3 att personlig integritet är den delen av säkerhet som folk tänker mest på, och menar att den aspekten är prioriteras framför att användning IoT enheter för att förstöra för andra. Vidare uttrycks att generellt så är personer inte medvetna om vilken slags information de delar med sig, och anser att etiska beslut är en viktig faktor som företagen idag och i framtiden måste ta itu med. Vad som menas med etiska beslut tar respondent 3 upp ett exempel gällande ökandet av självkörande bilar och understryker att även om det kan finnas risk med mjukvaran, så är inte människan ofelbar heller.

Som bra praktexempel på åtkomst till personliga uppgifter via Internet of Things berättar respondent 3 om utrustning för hjärtövervakning, som är en del av hela IoT, där en patient trycker in sitt personnummer och med det får man alla uppgifter gällande den patienten.

Det är intressant hur respondent 5 beskriver att idag delar mycket folk med sig av allt möjligt av sina liv på sociala medier samtidigt som de kommer och tycker att det är ett problem i samhället och menar att information om en själv sprids okontrollerat. Han menar på att detta är en konflikt som man måste lösa först innan man kan ta itu med den frågan på allvar.

Kostnad

Det finns nästan alltid en ekonomisk bakgrund gällande säkerhet menar respondent 1 och 2. Kostnaden definierar säkerheten anser respondent 4 och berättar att säkerhet är som kvalite, beror på vad kunden är beredda på att betala och det är inte förrän någon attack mot säkerheten inträffar som kunden är beredd att betala och då är det redan försent. Respondent 3 säger att tekniken finns för att kunna säkerhetsställa enheter, men att det är kostnad som är ett stort hinder, och menar ju mer tillförlitlig säkerhet, desto högre blir kostnaden. Vidare tänker man att detta är en av de större frågorna, om kunden är villig att betala för säkerhet eller inte.

När det kommer till kostnaden av vad en attack skulle kosta för ett företag där en hackare utför till exempel en DDoS attack för att utpressa ett företag kan vara förödande. Beroende på företagets storlek kan det handla om flera miljoner per dag då deras system ligger nere eller information är onåbar. Respondent 4 tar upp Amazon som exempelvis skulle förlora flera miljoner per dag. Ingen skulle bry sig om säkerheten om det inte finns någon ekonomi i det menar alla respondenterna.

Respondent 5 och 3 menar på att en stor anledning till varför företag väljer att inte fokusera på säkerhet från början är för att de ska kunna få ut sina produkter så snabbt som möjligt på marknaden. Företag, om de får välja, väljer hellre att få ut sin osäkra produkt snabbt på

marknaden än att vänta några år för att kunna leverera en säker produkt, detta för att säkerställa att man inte försvinner från marknaden.

Kostnaden finns även för attackeraren. Respondent 4 förklarar att för att knäcka en produkt, vilket inte är omöjligt idag, är kostnaden beroende på vilken typ av verksamhet man vill attackera och vilket pris informationen är värd. Mindre företag kostar mindre att attackera då de ofta finns luckor i säkerheten medans större verksamheter och myndigheter har färre säkerhetsluckor samt mer budget för sådana fall. Ska en attackerare göra en DDoS attack är kostnaden idag mindre för man kan kontrollera flera IoT-enheter än förut då attackeraren behövde ha tillgång till många datorer för att få ut den stora mängden datatrafik till attackytan.

4.2.3 Konsekvenser

Säkerhetsattacker

Medvetenheten av säkerhetsbrister ökar i takt med att mängden säkerhetsattacker ökar, enligt respondent 3 och hänvisar till attacker som Denial of Service som kan slå ner massvis med webbsidor genom små inbyggda datorer i produkter. När det gäller var säkerhetsrisker finns i IoT-infrastrukturen berättar respondent 4 att det helt beror på vad man vill attackera, vill man göra en överbelastningsattack är det själva mängden av end-noder som är intressant. Däremot om man vill åt skyddsvärd information som patientinformation eller annan personlig information kan det vara i molnet och databaser vilket betyder att endast en enhet kan räcka för att man ska hitta säkerhetshål i mjukvaran.

Ett exempel som respondent 3 tar upp gäller ett stort, världsledande belysningsföretag som blev utsatta för en drönarattack. Genom en video som spreds via media, fick man reda på att företaget på sitt kontor använde sitt egna ‘smarta’ belysningssystem som de benämner som personligt och trådlöst. Därefter såg man en tydlig inspelning på hur det utanför deras kontorsbyggnad flög förbi en drönare, och för varje fönster som drönaren flög förbi så släcktes lampor. Någon hade alltså lyckats att ta sig in på belysningsföretagets server och kunnat styra deras belysningssystem. Med detta exempel kunde man tydligt förstå hur alla enheter som förknippas med Internet of Things kan användas för att utsätta andra enheter för intrång. I just detta fall var det ingen skada som blev skedd, men denna typ av intrång kan användas för en potentiell, mer farlig attack.

Respondent 4 berättar att hittar man en säkerhetslucka i en IoT-enhet med en viss mjukvaruversion kanske det finns 10 miljoner enheter som kan letas upp och kopplas ihop, modifieras och sen vara en del i en ‘zombiearmé’. Respondent 4 berättar vidare om att det kommer finnas miljarder sådana enheter som potentiellt kan sänka företag och till och med länder. Idag behöver man bara ha en enkel telefon för att slå ut ett helt Windows-nätverk och det behöver inte handla om särskilt mycket trafik för om vet man exakt hur man ska göra, kan man vara väldigt elak, menar respondent 4.

Respondent 5 berättar att eftersom en öppen källkod ligger publikt för alla innebär det att en hel del objekt innehåller samma kärnkod, med en viss funktionalitetskillnad, som vidare leder till många säkerhetsrisker. Samtidigt som kärnkoden kan dubbelkollas för säkerhetsbrister av flera utvecklare kan också hackare samarbeta för att hitta säkerhetshål i koden. På grund av att många enheter innehåller samma kärnkod kan hackers hacka flera miljoner enheter om de lyckas att

knäcka koden. Förutom det nämner också respondent 5 att samma sårbarhet som finns i en öppen källkod kommer även att finnas i en kod som man skapar själv från grunden. Skillnaden är bara att den koden inte kommer ligga publikt.

En annan intressant sak som respondent 5 nämner är att många av de attackerna som sker idag har sedan långt tillbaka funnits, problemet är att man faktiskt inte tar tag i bristerna och fixar dem. Respondent 5 säger även att många företag fortfarande skickar okrypterad information även fast vi vet, sedan 60-talet att det är farligt och anser därmed att det finns en stor kunskapsbrist inom det.

4.2.4 Åtgärder

Respondent 1 beskriver säkerhet som ”Säkerhet är ingenting man har – det är någonting man gör.” Vidare beskriver respondent 1 och även 2 att de håller utbildningar för deras anställda gällande hantering av säkerhet och risker samt arbetar proaktivt med hantering av säkerhetsrisker genom deras interna säkerhetsteam. De tar också upp ett exempel på ett företag som har haft högt säkerhetstänk gällande deras IoT produkter, nämligen IKEA. IKEA gjorde så kallade “smarta lampor” och för att kunna säkerställa att lamporna var säkra deltog IKEA i en konferens för hackare (Sec-T) och bad dem att försöka hacka lampan. Säkerhetstänket hos IKEA prioriteras högt då de väljer att testa sina produkter först innan de kommer ut på marknaden detta gör i sin tur att de slipper kalla tillbaka alla produkter på grund av säkerhetsbrister. Respondent 4 menar att säkerhet har med tillit att göra. Har man då en gång hanterar det dåligt ät det svårt att få tillbaka tilliten, vilket är en konsekvens av säkerhetsbrister i ett företags IoT-enheter.

På u-blox nämner både respondent 3 och 4 att man använder sig av Secure boot, vilket är ett av deras koncept som ser till att det enbart är mjukvaran som u-blox skapat som kan köras, och skulle någon försöka hacka sig in utifrån så stängs enheten automatiskt av. u-blox arbetar tillsammans med andra säkerhetsföretag som är uteslutande experter för att se till att deras produkter kan stå emot attacker. Detta eftersom deras specialistkunskap är på deras produkter och även om säkerhet är en del av det så arbetar dessa säkerhetsföretag uteslutande med att hålla koll på marknaden och senaste säkerhetsattacker och kan därför ge den bästa rådgivningen, berättar båda respondenterna från u-blox.

Respondent 3 berättar även om End-to-End security, som är en av de mest välanvända metoderna för att säkerhetsställa förbindelsen mellan olika enheter. Genom End-to-End ser man till att kunden ska kunna skicka ut data från sin enhet ut till molnet, och kanske vidare, och se till att att man inte ska kunna bryta den länken någonstans ‘på vägen’. Det är något som man använder på majoriteten av sina produkter på u-blox länge, då de är ett företag som alltid varit duktiga på att säkerhetsställa förbindelsen ‘via luften’.

Respondent 4 berättar om att u-blox utgår från CIA “Sen har säkerhet tre saker, en triad, det ska vara confidentiality, integrity och availability. Och det är hela tiden en balansgång.”

Enligt respondent 5 så är det vanligaste sättet att säkerställa att informationen inte sprids, genom att använda kryptering, detta för att skydda informationen som enheten innehåller eller har tillgång till. Detta menar även respondent 4 som förklarar att man gärna vill använda sig av

kryptografisk säkerhet därför att det är väldigt svårt att bryta och ingen har kommit på hur man gör det än för man använder säkra nycklar och säkra nyckellängder. Däremot går hårdvaran att knäcka.

4.2.5 Framtiden

Samtliga respondenter anser att säkerhet lär vara en självklarhet inom den teknologiska utvecklingen och att det är dags att det prioriteras. Inom IoT anser samtliga att utvecklingen har gått så pass snabbt att säkerheten i många fall inte prioriterats och detta leder till problem. Respondent 3 emfaserar däremot på att vi bara är i början på eran av Internet of Things, att det enbart blir mer och mer. På plats uppskattar man att mängden IoT enheter möjligtvis kan hamna uppemot 100 miljarder enheter.

Respondent 4 anser att de måste göra det lättare för kunderna att skydda sig, i takt med att chippen blir mer och mer avancerade då det tillkommer mer säkerhetsfunktioner. Han hävdar att de borde ha metoder för att uppdatera deras kunder *när* en läcka händer och inte om det händer. Han beskriver att det handlar om att hitta säkerhetsluckorna och täppa igen dem.

Respondent 3 berättar att man på u-blox bland annat jobbar med säkerhet genom att ha en mer än nödvändigt lång krypteringsnyckel. Men han berättar att man i framtiden förväntar sig en utveckling av någon sorts kvantmekanisk dator. Vid ett sådant tillfälle kan man helt bortse från de nuvarande metoderna för kryptering, då en kvantmekanisk dator lär kunna hacka allt genom en enorm datorberäkningskraft som jobbar operativt med att lösa algoritmerna.

Enligt respondent 5 kommer funktionalitet alltid att vara drivande men efterhand som säkerheten blir viktigare i takt med att sårbarheterna blir mer och mer omfattande kommer intresset för säkerhet växa. Respondent 5 berättar att i framtiden kommer inte en person att drabbas vid en attack utan då kommer hela städer eller nationer att påverkas och menar på att konsekvenserna är värre idag än vad de var förr och kommer att fortsätta att bli värre och värre i takt med att tekniken allt blir mer omfattande.

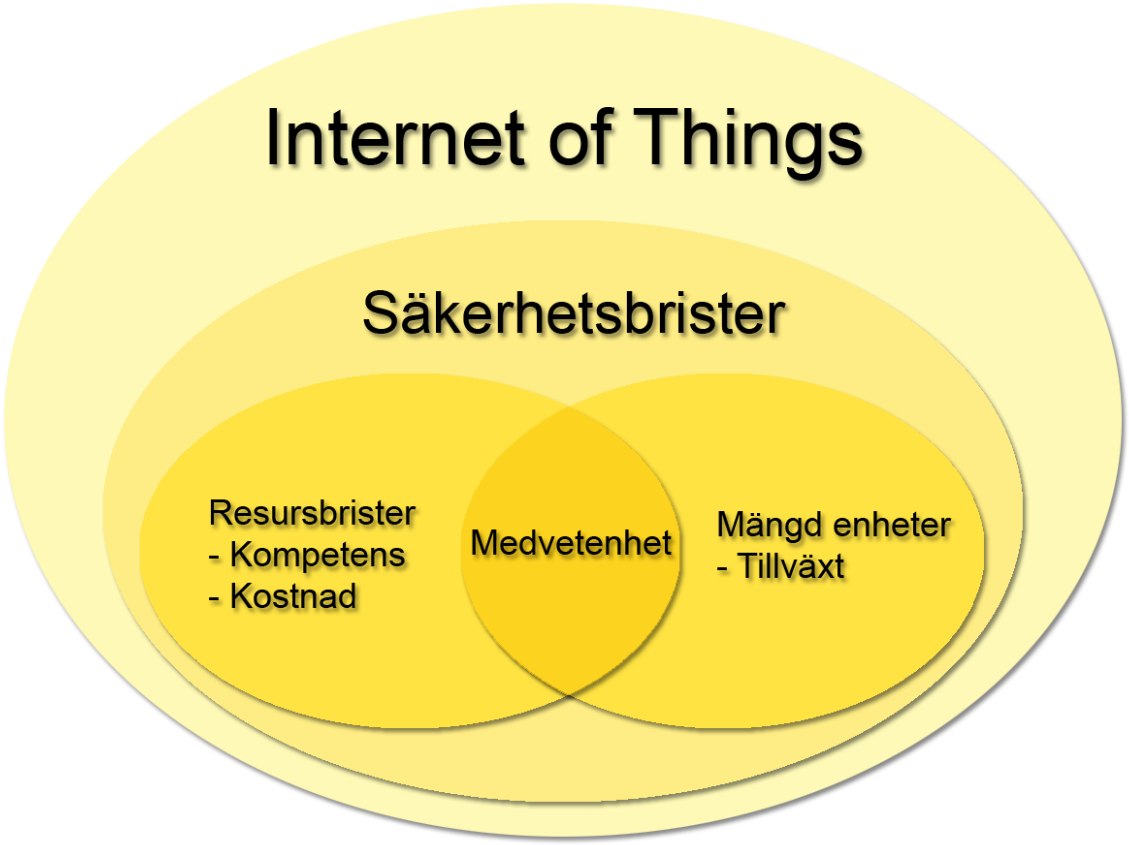
Respondent 3 är övertygad om att i framtiden kommer det finns en övervägande del av självkörande bilar, och även om man idag är skeptisk till potentiella olyckor, så kommer säkerhetsteknologin utvecklas i snabb fart. Redan idag formas organisationer som består enbart av professionella hackers som fokuserar på att testa olika företags produkter för att kunna säkerhetsställa både den funktionella och säkerhetstäta delen. På u-blox säger respondent 3 att detta är ett arbetssätt men nyligen börjat jobba med, och som man tror lär vara en självklar del av andra företags arbetssätt.

Samtliga respondenter menar på att kunskapen om ett säkrare IoT-samhälle finns, men den används inte än och den måste bli större. Man menar på att det inte är så många som besitter den kunskapen och vad som istället krävs är utbildning. Vidare säger även respondent 3 att i en ny era av Internet of Things och diverse nya tekniker så kommer nya lagar och standarder att öka radikalt, med exempel på den nya regleringen från EU som kallas för General Data Protection Regulation (GDPR). Kunder lär nämligen ha krav på att alla variationer av enheter kommer att uppfylla en viss, specifik standard.

5. Diskussion

I diskussionsdelen jämför vi teori med den insamlade empirin. Med våra personliga erfarenheter och tankar har vi tolkat och hittat samband och olikheter mellan teorin och empirin.

Genom att undersöka de teoretiska perspektiven som drivits av det senaste tekniska säkerhetsaspekterna tillhandahölls en grundlig förståelse hur IoT har utvecklats och tekniken bakom IoT genom det olika skikten i infrastrukturen. Vidare hanterades säkerhetsaspekter från CIA-triaden, känd som den grundläggande säkerhetsförståelsen av utövare och akademiker. De empiriska resultaten fokuserade mycket på medvetenheten om säkerhetsbrister inom IoT och företags upplevelse av detta. Däremot har det visats att företag nu är medvetna om att det finns säkerhetsbrister men att de inte riktigt vet hur dessa ska tacklas. Resultaten från den empiriska studien har lett till att vi har identifierat faktorer som leder till säkerhetsbrister i IoT-enheter som företag bör överväga. Genom att understryka *medvetenhet* som nyckelfaktor, följt av *resursbrist* och *mängd enheter* visar detta på vad företag bör överväga. I resursbrist har två delfaktorer identifierats nämligen kompetens och kostnad. Vidare har även mängd enheter tillväxt och privacy som delfaktorer. Figur 4 nedan presenterar dessa faktorer i relation till varandra.



Figur 5: Säkerhetsbrister i relation till IoT

Resursbrist

Kompetens

Vi har genom studien sett att kompetensen för att skapa säkra IoT-enheter finns men, det är för få som besitter den. Det visar sig, både i teorin och i empirin att det saknas säkerhetstänk i utbildningen men enligt empirin är det på väg att bli ett mer populärt ämne för studenter. Att det dessutom lider brist på cirka 750 000 utvecklare i EU bidrar till att det förmodligen kommer att bli en enormt brant backe upp för att kunna täcka alla positioner.

Samtliga respondenter är eniga om att utbildning i både skolor och på företag behövs för att kompetens ska kunna spridas i den takt som behövs idag. Alla behöver inte bli experter på säkerhet men det krävs att alla är medvetna om att det kan vara en fara och då kanske frågar en extra gång istället för att ta ett beslut helt okunnig. Att bara vara medveten om risker som finns skapar en ökad säkerhet.

En annan viktig faktor till varför säkerhet har kommit i efterhand är för att företag har lagt fokus på andra kompetenser som till exempel funktionalitet och design. Detta är även sakerna som säljs idag, det som kunden tittar på när de väljer, vilket skapar en ond cirkel. Företagen väljer att prioritera bort säkerhet eftersom kunderna ändå inte är medvetna om att det är så viktigt, de vill hellre ha en cool pryl som är snygg. Förhoppningsvis kommer detta att vända. Enligt respondent 3 kommer det förmodligen att vända i takt med att det sker fler och fler attacker mot prylar så kommer säkerhet tillslut att efterfrågas av konsumenterna och då kommer företagen att tvingas att skapa säkra produkter.

Kostnad

Med hänvisning till problemformuleringen tidigare i denna uppsats skriver Gartner (2017) att IoT kommer stå för mindre än 10 procent i företags IT-säkerhets budget, vilket vi tycker är mycket oroväckande. Alla respondenter berättar att storleken på företag kan spela stor roll för vad de väljer att prioritera. Större företag tenderar att fokusera mer på säkerheten eftersom de har resurserna och dessutom har mycket att förlora om de skulle tillverka IoT-enheter som senare visar sig vara osäker. Ett företag som har lagt stort fokus på just denna typ av säkerhet är IKEA, det märks tydligt i det exemplet om deras smarta lampor som respondent 1 och 2 beskriver. Detta till skillnad från mindre företag, där det är viktigare att synas snabbt på marknaden och växa vilket kan leda till att de producerar osäkra IoT-enheter. Företag, stora som små, som är specialister på en specifik sak exempelvis sjukhus, advokatbyråer och så vidare kommer diskuteras mer under punkten medvetenhet.

Att använda sig av öppen källkod, kod som är publicerad publikt, handlar oftast också om att det är kostsamt men även tidskrävande för företag att utveckla en helt egen kod från grunden. Fördelen med öppen källkod är precis som Vadalasetty (2003) och respondent 5 beskriver att många kan hjälpas åt att hitta hål eller sårbarheter i koden och nackdelen är att om en hackare lyckas med att hitta ett hål eller en sårbarhet i koden kan denne ta sig in i många miljontals enheter just eftersom de delar samma kärnkod. Ytterligare en nackdel gällande öppen källkod är precis som Karalov (2018) beskriver att när företag väljer en öppen källkod, dubbelkollas den inte för eventuella sårbarheter då de tror att den är säker. Vidare är det värt att nämna att det också kommer att finnas hål eller sårbarheter i en egenutvecklad kod men då blir frågan, hos

hackare, vad är värt att attackera? En enhet, eller flera miljontals enheter? Många hackare väljer att göra intrång flera enheter trots att det är flera gånger svårare eftersom idag handlar det mer och mer om pengar.

Som nämnt ovan gällande kompetens vill vi också belysa här, att fokus på funktionalitet och design också går hand i hand med kostnader. Respondent 3 menar på att många kunder tidigare prioriterat funktionalitet framför säkerhet, då det är funktionalitet som säljer. Många företag vill heller inte vänta med att få ut sina enheter på marknaden. De släpper hellre en enhet snabbt som inte har komplett säkerhet än att vänta. Detta i sin tur leder till det som Li & Da Xu (2017) påstår, att mängden enheter ökar snabbt därmed också okontrollerat.

Mängd enheter

Tillväxt

En självklarhet med Internet of Things, och även ett av dess största problem, är mängden enheter som ökar snabbt. År 2017 uppskattade Gartner (2017) att mängden enheter skulle hamna på 20 miljarder enheter, men redan år 2018 lyckades man redan nå denna mängd. Nu pekar istället det internetbaserade statistikcentret Statista att det idag finns strax över 23 miljarder uppkopplade IoT-enheter, och att man beräknar 24 miljarder enheter år 2020. Med dessa olika förutsägelser kan man göra antagandet att mängden enheter i framtiden är svår att precisera, och att vi enbart är i en tidig fas i eran av Internet of Things.

I takt med att mängden enheter ökar, ökar även en oro bland företag som till slut kommer att inse att det blir ett påtagligt problem. Man menar att de hot som finns idag, enbart kommer bli värre. Även om tekniken för säkerhetslösningar även den utvecklas snabbt, så blir det en konstant tävling mellan dessa utvecklare och hackarna. Med Holmbergs (2016) hänvisning till Moore's lag förklaras det tydligt att i och med en exponentiell utveckling av tekniken som blir allt mer kraftfull, att säkerhet har blivit och framförallt kommer ha en stor del av våra liv. Internet of Things är ett praktexempel på Moore's lag, men är ett fenomen vars säkerhetsaspekt är gravt förbisedd av många företag.

u-blox är ett av de företag som i tidigt skede försökt att ha ett kontinuerligt säkerhetstänk och förutsåg komplexiteten av Internet of Things. Där har man tydligt sett ett mönster mellan mängden enheter och säkerhetstänket bland deras kunder. Det har uppstått en tydlig trend bland deras kunder, och även företag i allmänhet, att prioritera säkerhet allt mer. Detta dels för att man börjat förstå de allvarligare konsekvenser av att koppla upp allt fler enheter mot internet. Tillverkningen av framtida uppkopplade enheter sker ju i miljontals exemplar, och skulle dessa användas för att potentiellt intrång skulle det ha stor skada på både organisationer och internet på grund av den stora mängd trafik som kommuniceras fram och tillbaka. Många enheter har samma mjukvara i sig och om den går att hacka finns det chans att skapa en hel arme av enheter, beskriver respondent 4 det som. Med tanke på ökningen av enheter blir både organisationer och individer utsatta för en stor risk vid en eventuell attack.

Privacy

För att organisationer ska kunna genomföra täta säkerhetsåtgärder, är det väsentligt att de är vaksamma på den snabba utvecklingen av både teknologin och mängden enheter. Genom en oförmåga att faktiskt förstå Internet of Things och dess komplexitet var en av anledningarna till varför en sådan stor säkerhetslucka uppstod. Genom enheterna kan man både får åtkomst till andra uppkopplade enheter, samt den information som ligger lagrad på samma nätverk som enheten. Detta är känt som två viktiga områden inom CIA, IoT Security och IoT Privacy, Rouse (2014) beskriver skillnaden mellan IoT privacy och IoT security och belyser detta som några av CIA största utmaningar. Empirin visar att säkerhetsbristerna som respondenterna beskriver går att kategoriseras på två sätt, nämligen som problemområden inom privacy eller security, samt att det skiljer sig mellan dessa. IoT Privacy handlar om personlig integritet gällande IoT-enheter och vad som krävs för att skydda den privata informationen (Rouse, 2014). IoT security syftar på det stora antalet uppkopplade enheter och problematiken gällande säkerhetsproblem som överbelastningsattacker. Alla respondenter nämnde en eller flera säkerhetsproblem som kan kategoriseras som antingen IoT Privacy eller IoT Security, vilket gör att empirin går att ansluta till teorin om CIA (Rouse, 2014)

Medvetenhet

Alla respondenterna är medvetna om *att* det finns säkerhetsproblem som tillkommer vid användandet av IoT-enheter men frågan är om de är medvetna om *vilka* säkerhetsbrister IoT-enheter har som finns i deras närhet. Vidare är respondenterna själva medvetna om att många av deras kunder inte är medvetna om säkerhetsrisker gällande IoT-enheter.

Ett exempel på detta tar respondent 3 upp då han menar på att många kunder tidigare prioriterat funktionalitet och design framför säkerhet, då det är funktionalitet och design som säljer. Då kan företaget mycket väl vara medvetna om att det finns säkerhetsproblem gällande deras IoT-enheter men inte vara medvetna om hur förödande konsekvenser som kan uppstå i exempelvis en attack mot deras produkter. I detta fall handlar det om kostnader och medvetenheten om vad som är skyddsvärt och ekonomiskt värt att lägga resurser på.

Vidare, menar alla respondenterna att det är skillnad på företag och företag. Ett stort företag har oftast större resurser att lägga på säkerheten vilket gör säkerhetsarbetet enklare och mer omfattande. Även företag med speciell inriktning är mer medvetna om säkerhetsproblem nämner respondenterna 1, 2 och 3 samt tog upp exempel som advokatbyråer eller sjukhus, ställen där informationen verkligen måste hållas säker och där säkerhetstänket redan är implementerad i verksamheten. I de företagen är säkerhet en del av själva företaget vilket faller sig naturligt att man har väldigt hög säkerhet. Respondent 3 och 5 menar på att medvetna företag oftast i sin tur har specifika anställda som endast arbetar med säkerhet.

Ett exempel som motsäger detta är det kända belysningsföretaget när någon hade hackat sig in och tagit kontroll över lamporna på deras kontor och kunde släcka hela kontoret bara med hjälp av en drönare. Trots att man är ett stort företag med hög medvetenhet kan säkerhetsbrister finnas. Detta menar på, precis som respondent 3 förklarar, att medvetenheten ökar i takt med att säkerhetsattacker ökar samt att ett stort och så kallat *medvetet* företag kan bli utsatt för så pass simpla attacker.

Hackares kunskap utvecklas i takt med att tekniken utvecklas vilket leder till att det uppstår en kamp där säkerheten hänger inte med. Företag måste hela tiden sträva efter att ligga steget före när det gäller säkerheten i deras IoT-enheter. Ett bra exempel på detta är när IKEA bad hackare försöka göra intrång i deras smarta lampor. Detta visar på högt säkerhetstänk från ett företag och vikten av att ligga steget före för att motverka säkerhetsattacker. Respondenterna 3 och 4 nämner att de måste ligga steget före i deras säkerhetsarbete och i deras fall gäller det att kryptera i längre nyckellängd än vad datorer inte är kraftfulla nog att bryta.

6. Slutsatser

I denna studie har vi antagit utmaningen att förstå den nuvarande IoT-infrastrukturen och säkerhetsfrågor som uppstår kring detta. Efter att ha definierat vårt problemområde har vi diskuterat hur viktigt det är att säkerhetsfrågan inte får förbises, utan snarare beaktas, särskilt med tanke på att Moore's lag bevisar hur mängden enheten hela tiden ökar exponentiellt. Då IoT fortfarande är ett nytt fenomen, är det inte högt prioriterat hos företag vilket vår kvalitativa studie har visat. Dock kan man tydligt se att många företag, är medvetna om säkerhetsbristerna som IoT-enheterna kan skapa och den medvetenheten blir allt mer omfattande.

Forskningsfrågan som vi valde att undersöka i denna studie:

Vilka faktorer bör företag överväga gällande säkerhetsbrister i IoT-enheter?

Genom den teori och empiri som samlats in för att kunna besvara frågeställningen har vi kommit fram till att det är skillnad på medvetenheten beroende på företagstyp. Stora företag tenderar att vara mer medvetna precis som nischade företag som har högt säkerhetstänk inbyggt i verksamheten på grund av arbete med känslig information. Mindre eller nystartade företag har ofta inte resurser för att prioritera säkerheten framför att expandera på marknaden. Eftersom det idag är framförallt funktionalitet och design som säljer väljer många företag att fokusera på detta istället för säkerhet. I takt med att det sker fler attacker samtidigt som att utbildningen inom säkerhet blir mer omfattande, blir företag mer medvetna om värdet att fokusera på säkerheten. Ytterligare en konsekvens av att fokus framförallt ligger på funktionalitet och design är att mängden osäkra enheter ökar hastigt. Däremot anser vi att medvetenhet ligger till grund för ett lyckat säkerhetsarbete, och menar att det är av högsta grad viktigt att företag inser vikten av att vara medveten. Faktorerna som företag främst bör överväga, gällande säkerhetsbrister i IoT-enheter, är följande:

Medvetenhet	**Resursbrister** Kompetens Kostnad	**Mängd enheter** Tillväxt Privacy

Medvetenhet var den faktor som vi från start valde att utforska och har bevisats vara den faktorn som är anledningen till att de andra faktorerna uppkommit. Främst gäller det att man som företag är medveten, inte bara över de tekniska trenderna, men framför allt de samtliga säkerhetsrisker som tillkommer för just deras företag.

Resursbrister resulterades i en kategorisering av "Kompetens" och "Kostnad", då studien visade dessa som stora brister inom själva företagen. Det menas på att man antingen inte har den spetskompetens som krävs för att utveckla, och hänga med i vad man imorgon kommer kunna se som fullständigt nya metoder inom både IT-säkerhet och programmering. Heller har man inte de finansiella resurserna för att se till att sina produkter är tillräckligt säkra. Tekniken finns där, men inte pengarna.

Mängd enheter har varit anledningen till varför problemet har blivit så uppmärksammat, så snabbt. Ingen av den undersökta statistiken har tidigare förutspått rätt gällande mängden enheter under ett visst årtal. Istället har mängden varit avsevärt mycket större än vad man förväntat sig, och genom en analys av detta blir framtiden av IoT-enheter relativt oförutsägbar vilket i sig kan skapa en osäkerhet. Som ett resultat av detta utsätts inte bara organisationer för potentiellt större intrång, men även individer som är omringade av uppkopplade enheter. Frågan gällande privacy blir allt större, genom att individer blir påverkade.

Samtliga faktorer har genom vår kvalitativa studie upprepats ett flertal gånger, både genom teorin, empirin samt vår diskussion. I den snabbt växande industrin som IoT är verksam i, har det varit avsevärt tydligt att det flera utmaningar väntar. Med vår undersökning och slutsats är det tydligt att faktorerna nämnda ovan är några av dessa utmaningar, men som tidigare diskuterat är Internet of Things enbart i början av sin era och att vägen som är utlagd framför många företag är lång att gå.

6.1 Förslag på vidare arbete

Med tanke på att vår studie har varit fokuserad i ett svenskt sammanhang, och att vi enbart undersökt organisationer som på något vis redan arbetar med Internet of Things, anser vi att vår studie kan göras om och gå ännu djupare in på två olika vis. För det första bör framtida studier på detta vis inkludera fler länder. Vi anser att kulturella skillnader, lagar och dylikt kan driva flera organisationer i andra länder att vara strängare med säkerheten. För det andra menar vi att förlängningen av vår studie mot slutanvändare och deras medvetenhet om säkerhetsfrågor är mycket relevant för framtiden för Internet of Things och dess engagemang i samhället.

7. Referenser

Aazam, M., Khan, I., Alsaffar, A. A., & Huh, E. N. (2014). Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved, *Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference on* (pp. 414-419). IEEE.

Abomhara, M., & Koien G. M., (2014) Security and Privacy in the Internet of Things: Current Status and Open Issues, *IEEE*

Agarwal, A. & Agarwal, A., (2011). The Security Risks Associated with Cloud Computing, *International Journal of Computer Applications in Engineering Sciences*

Bisson, D., (2018). One in Five Healthcare Employees Would Be Willing to Sell Sensitive Data, Reveals Survey, *The State of Security*, 9 mars, Tillgänglig online: https://www.tripwire.com/state-of-security/latest-security-news/one-in-five-healthcare-employees-would-be-willing-to-sell-sensitive-data-reveals-survey/ [Hämtad 26 mars 2018]

Botta, A., de Donato, W., Persico, V., Pescapé, A., (2016) Integration of Cloud computing and Internet of Things: A survey, *University of Napoli Federico II, Italy.*

Brooks, C. (2015, June). "How Safe Do Your Employees Feel?" *Business News Daily,* 26 juni, Tillgänglig online: https://www.businessnewsdaily.com/8139-keeping-employees-safe.html [Hämtad 2 mars 2018]

Chavan, A. & Nighot, M., (2014) Secure CoAP Using Enhanced DTLS for Internet of Things, *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 2, issue 12

Eastwood, G., (2017). 4 critical security challenges facing IoT, *Networkworld*, 7 februari, Tillgänglig online:https://www.networkworld.com/article/3166106/internet-of-things/4-critical-security-challenges-facing-iot.html [Hämtad 19 april 2018]

Gartner (2018). Tillgänglig online: https://www.gartner.com/it-glossary/internet-of-things/. [Hämtad 18 april 2018]

Gartner (2017). Leading the IoT: Gartner Insights on How to Lead in a Connected World [pdf]. Tillgänglig online: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf [Hämtad 18 april 2018]

Gollmann, D. (2011). Computer Security, 3rd ed. IN: *John Wiley and Sons.*

Guarda, T., Fernanda, M., Haz, L., de la Cruz, M., Orozco, W., Alvarez, J., (2017) Internet of

Things challenges, *Proceedings of the 12th Iberian Conference on Information Systems and Technologies,* Tillgänglig online: https://www.researchgate.net/publication/318415208_Internet_of_Things_challenges [Hämtad 18 april 2018]

Harris S (2002). CISSP Certification Exam Guide. *McGraw-Hill/Osbourne*

Holmberg, C. (2016) Vad är Moores lag? *Nordichardware*, 23 mars, Tillgänglig online: https://www.nordichardware.se/test/vad-ar-moores-lag.html [Hämtad 2 april 2018]

Hughes, R. D. (2015). Two concepts of privacy, *Computer Law & Security Review: The International Journal Of Technology Law And Practice*. Tillgänglig online: https://ac.els-cdn.com/S0267364915000904/1-s2.0-S0267364915000904-main.pdf?_tid=eb3699f6-15e7-469f-bf12 a191cfd64ee5&acdnat=1526294093_a4ecb149019184dabb1d545774d3e3bf [Hämtad 22 april 2018]

IBM builds a smarter planet (2018). Tillgänglig online:http://www.ibm.com/smarterplanet/us/en/ [Hämtad 18 april 2018]

Jacobsen, D. I., (2002). Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Lund, Studentlitteratur.

Jaffey, T (2014) MQTT and CoAP, IoT Protocols, *Eclipse Foundation*, Tillgänglig online: https://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php [Hämtad 22 april 2018]

John N. A., (2012) Sharing and Web 2.0: The emergence of a keyword. *The Hebrew University of Jerusalem*, Israel

Karalov, M. (2018) Open source software security challenges persist, *CSO from IDG*, Tillgänglig online: https://www.csoonline.com/article/3157377/application-development/open-source-software-security-challenges-persist.html [Hämtad 2 maj 2018]

Vahid Dastjerdi, A., and Buyya, R., (2017) Internet of Things: Principles and paradigms, Morgan Kaufmann Publishers

Kumar, J & Patel, D. (2014) A Survey on Internet of Things: Security and Privacy Issues *International Journal of Computer Applications* (0975 – 8887) Volume 90 – No 11, 3 mars, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7902207 [Hämtad 19 april]

Kvale, S. (1996). Interviews: An Introduction to Qualitative Research Interviewing, London: Sage.

Lantz, A. (2007). Intervjumetodik, 2: a. uppl, Lund, Studentlitteratur.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons.* Tillgänglig online: http://iranarze.ir/wp-content/uploads/2016/10/E2609.pdf [Hämtad 1 april]

Li, S., & Da Xu, L. (2017). Securing the internet of things. Syngress Publications.

Malmqvist, M., (2016) Så många miljoner nya prylar kopplas upp - varje dag. *Computer Sweden,* 8 mars, Tillgänglig online: https://computersweden.idg.se/2.2683/1.650672/uppkopplade-prylar-iot [Hämtad 18 april]

Mohamed, A. (2008) Open source software security. *Computer Sweden,* 1 april, Tillgänglig online: https://www.computerweekly.com/feature/Open-source-software-security [Hämtad 2 maj 2018]

Nilsson, M., (2016) Uppkopplade prylar kräver säkra nät, *Tele2*, 10 februari, Tillgänglig online: http://betterbusiness.tele2.se/2016/02/glom-inte-sakerheten-hos-dina-uppkopplade-prylar/ [Hämtad 14 april]

Novotek. (u.å). IoT Gateway med REST och MQTT interface. Tillgänlig online: https://www.novotek.com/sv/l-sningar/kepware-opc-kommunikationsplattform/iot-gateway-med-rest-och-mqtt-interface [Hämtad 12 april 2018]

Olsson, H., Sörensen, S., (2011) *Forskningsprocessen: kvalitativa och kvantitativa perspektiv*. 3. Uppl. Stockholm

Olzak, T. (2017) IoT messaging protocol is big security risk. Opinion: Olzak on business continuity. Tillgänglig online: https://www.csoonline.com/article/3207770/internet-of-things/iot-messaging-protocol-is-big-security-risk.html [Hämtad 23 april 2018]

Sethi, P. & Sarangi, S., "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering, vol. 2017

Post, J. (2016). Before Disaster Strikes, You Need a Business Continuity Plan. Business News Daily, 1 september. Tillgänglig online: https://www.businessnewsdaily.com/6059-disaster-recovery-planning.html [Hämtad 1 mars 2018]

Ripeanu, M. (2001). Peer-to-Peer Architecture Case Study: Gnutella Network. Tillgänglig online: http://people.cs.uchicago.edu/~matei/PAPERS/gnutella-rc.pdf [Hämtad 15 mars 2018]

Rouse, M. (2016). Tillgänglig online: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [Hämtad 19 april 2018]

Rouse, M. (2014). Tillgänglig online: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA [Hämtad 19 april 2018]

Sentor (u.å), Tillgänglig online: https://www.sentor.se/kunskapsbank-it-sakerhet/ddos-attack/. [Hämtad 4 maj 2018]

Schaller, R. (1997). Moore's Law: past present, and future. Tillgänglig online: http://mprc.pku.edu.cn/courses/organization/autumn2013/paper/Moore's%20Law/Moore's%20law%20past,%20present%20and%20future.pdf [Hämtad 15 mars 2018]

Statista (2018. Tillgänglig online: https://www.statista.com/statistics/471264/iot-number-of- connected-devices-worldwide/ [Hämtat 4 maj 2018]

Thakare, S., Patil, A., & Siddiqui, A. (2016). The Internet of Things-Emerging Technologies, Challenges and Applications. *International Journal of Computer Applications*, *149*(10). Tillgänglig online: https://pdfs.semanticscholar.org/efb5/5011b3e2e29d95831b58c9819e7e198df33e.pdf [Hämtad 19 april 2018]

Thoresson, A., (2017) *Han ska göra uppkopplade prylar säkrare.* NyTeknik, 3 mars. Tillgänglig online: https://www.nyteknik.se/innovation/han-ska-gora-uppkopplade-prylar-sakrare-6825287 [Hämtad 4 maj 2018]

University of Washington Information School (2018). *What is informatics?* Tillgänglig online: https://ischool.uw.edu/programs/informatics/what-is-informatics [Hämtad 1 april 2018]

Vadalasetty, S., R. (2003) Security Concerns in Using Open Source Software for Enterprise Requirements. *SANS Institute.* Tillgänglig online: https://www.sans.org/reading-room/whitepapers/awareness/security-concerns-open-source-software-enterprise-requirements-1305 [Hämtad 2 maj 2018]

Wachter, S. (2018). GDPR and the Internet of Things: Guidelines to Protect Users' Identity and Privacy. Tillgänglig online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130392 [Hämtad 29 mars 2018]

Wachter, S. (2017). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, *Computer Law & Security Review, Forthcoming* Tillgänglig online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3083554 [Hämtad 29 mars 2018]

Weber, R. (2010). Internet of Things? New Security and Privacy Challenges, *26 Computer Law & Security Review 23* Tillgänglig online: https://www.sciencedirect.com/science/article/pii/S0267364909001939 [Hämtad 29 mars 2018]

Whitmore, A., Anurag A., and Da Xu, L. (2015) The Internet of Things--A Survey of Topics and Trends, *Journal Information Systems Frontiers, New York 261, 261* Tillgänglig online: https://dl.acm.org/citation.cfm?id=2750627 [Hämtad 4 maj 2018]

Witeck, C. (2016). The internet of things is in your future - the law says so!, *IoT Agenda, TechTarget*. Web blog post tillgänglig online: https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/The-internet-of-things-is-in-your-future-the-law-says-so [Hämtad 4 april 2018]

Yassein, M., Shatnawi, M., and Al-zoubi, D., Application layer protocols for the Internet of Things: A survey, *2016 International Conference on Engineering & MIS (ICEMIS)*, Agadir, 2016, pp. 1-4.

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges, *Security & Communication Networks.* Tillgänglig online: https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf [Hämtad 4 april 2018]

8. Appendix

Bilaga 1: Intervjuguide

Vilka faktorer bör företag överväga gällande säkerhetsbrister i IoT-enheter?

Vi har valt att fokusera på uppkopplade* IoT-enheter, inte datorer, surfplattor och mobiler utan kopieringsmaskiner, övervakningskameror, larmsystem och så vidare. Vi har upptäckt att säkerheten inte prioriteras i dessa produkter och vill utforska det ytterligare. Vi vill också utreda hur pass medvetna företag är om de risker som finns med uppkopplade enheter.

* Med uppkopplade produkter menar vi saker som är uppkopplade till internet. Produkter som skickar information till ett moln utan komplexiteten som en dator, surfplatta eller mobil har.

Inledande frågor

- Är det okej om vi spelar in?
- Vi presenterar oss och berättar om kandidatuppsatsen
- Intervjupersonen berättar om sig själv och sin yrkestitel
- Berätta lite om företaget/projektet?

Bakgrundstankar

- Medvetenhet
- Bild av säkerhet och säkerhetsbrister
- Konsekvenser
- Åtgärder

Del 1 - *Om intervjuobjektet har IoT-produkter i sin verksamhet*

- Anser ni att uppkopplade enheter är ett problem, dvs att de utgör en risk för potentiellt dataintrång eller för organisationen överlag? Varför?
- Vad för slags enheter har ni vardagligen uppkopplade till internetet?
- Vad gör ni för att säkerhetsställa att er information är säkert lagrat?
- Är du medveten om riskerna som finns med uppkopplade enheter?
- Hur arbetar ni med medvetenheten av säkerhetsrisker hos anställda i ert företag?
- Arbetar ni proaktivt med hantering av säkerhetsrisker? I så fall hur?

Del 2 - *Om intervjuobjektet arbetar i en verksamhet som tillverkar IoT produkter*

- Tillverkar ni uppkopplade produkter?
- Vilka krav ställer era kunder på säkerheten på era produkter?
- Är kunderna medvetna om att det kan finnas säkerhetsrisker?
- I vilken ordning prioriterar ni att era produkter är tillräckligt säkra?
- Vad gör ni som utvecklare av IoT-produkter för att se till att era kunder är medvetna om de risker som de kan potentiellt kan behöva bemöta?

Del 3 - *Om intervjuobjektet forskar inom IoT*

- Vad är din yrkestitel?
- Hur kommer det sig att du valt att fokusera på just den inriktningen (om den är IoT)?
- Du har jobbat med ditt projekt "Seconds". Vill du berätta lite om det?
- Säkerhet, skulle du säga att det är en "trend"? Varför blev den viktig bara för två år sedan? Personlig åsikt gällande säkerhetsbristen?
- Vad tror du är den underliggande anledningen till varför man inte prioriterat säkerheten?
- Hur tror du att framtiden kommer att se ut?

Teknik

- Vi har en bild hur ett IoT-system är uppbyggt med antingen en tre- eller femskikts arkitektur, som vi har förstått det som. Hur ser din bild av tekniken kring Internet of Things ut?

Bilaga 2: Intervju med Atea

Intervju med Christer Böke och Mikko Verlinna, säljspecialist inom säkerhet respektive verksamhetsutvecklare	
Datum:	05-04-2018
Tid	09.05-10.47
Intervjuare	Emma Nilsson, Matilda Stading, Victoria Andersson
Intervjuperson	Christer Böke och Mikko Verlinna

Nedan lyder en sammanfattning av intervjun med Atea 05-04-2018 baserat på de anteckningar som fördes under och direkt efter, samt inspelat material av de första 10 minuterna. Sammanfattningen är uppbyggd från en semistrukturerad intervju och svaren tillhör rubrikerna eftersom spontana frågor uppkom efter det bestämda frågorna från den bestämda intervjuguiden. Intervjun började med presentationer av respondenterna, Christer, Säljspecialist inom säkerhet i Malmö och Mikko, verksamhetsutvecklare i Eskilstuna. Christer och Mikko var tydliga med att deras svar var baserade på egna åsikter och upplevelser och representerar inte nödvändigtvis Atea.

Intervju

Om uppkopplade enheter inom Ateas verksamhet

Ja det har vi, men inte så många. Mer specifikt är tv-skärmar som visar erbjudande på alla kontor i Sverige, det kan anses som IoT. Vi har även kopieringsmaskiner som är uppkopplade till nätet. Det finns en "Print" avdelning som jobbar mot kunder och erbjuder print, dokumenthantering och liknande.

Om kunder och deras uppkopplade produkter inom sin verksamhet

Respondenterna fortsätter att förklara att många kunder använder sig av uppkopplade produkter. Bland annat deras tjänster från Print avdelningen. Men kunde inte säga om alla kunder hade det. Det beroende mycket på kunden.

Om kunder är medvetna om säkerhetsrisker gällande uppkopplade produkter

Gällande medvetenhet om de säkerhetsrisker som tillkommer med uppkopplade produkter svarade respondenterna att vissa kunder inte är medvetna. Det prioriterar inte alltid säkerhet. Däremot är större företag generellt mer medvetna. Atea hjälper kunder om de har krav gällande

säkerhet och försöker inte sälja på någon det. Respondenterna anser att kunder är generellt inte medvetna om sin IoT säkerhet och att det inte prioriteras. De berättar vidare att det också beror på verksamheten. De uppfattar att de kunderna som tänker mer på säkerhet brukar ha information som måste skyddas. Kan vara små företag men med högt säkerhetstänk som exempelvis en advokatbyrå där det prioriteras att hålla deras information säker. Däremot kan små företag, som till exempel tillverkande eller butiker ha lågt säkerhetstänk. Beror både på storlek och inriktning.
.

Ett exempel som togs upp var gällande printers, företagen som gör produkterna kan ha många säkerhetsfunktioner men kunder som har dessa produkter kanske inte aktiverar dessa likväl. Kan vara på grund av okunskap eller att kunden ej är medveten om riskerna och vilka möjligheter som erbjuds i den tekniska plattformen. Detta kan bero på hur moget företaget är gällande säkerhetsfrågor.

Respondenterna berättar vidare att deras kunder har ofta hela paketet som ATEA erbjuder. Det vill säga att de använder sig av alla tjänster ATEA erbjuder, allt från säkerhet till IT infrastruktur. Men ibland tar kunder in en tredje part som exempelvis testar eller är experter. ATEAs kunder prioriterar mestadels: perimeterskydd, filhantering, dataskydd, brandväggar och identitetshantering med flerfaktor autentisering.

Om vad man gör för att säkerhetsställa att information är säkert lagrat
Respondenterna förklarar att inom säkerhet är det vanligt med identitetshantering. Ett exempel som gavs var genom en liknelse med nycklar till rum. Det kan finnas många nycklar till många rum men man behöver inte ge alla nycklar till alla personer. Vissa rum behöver bara vissa ha tillgång till. Så därför är identitetshantering viktigt. Alla behöver inte komma in i alla system till exempel.

De förklarade också att Atea har utbildningar för anställda inom säkerhetsaspekter däremot mer generellt om säkerhet, lösenordshantering och liknande. Inte specifikt om IoT enheter.

Atea arbetar proaktivt med hantering av säkerhetsrisker. De har ett helt säkerhetsteam, egen krishantering och erbjuder kunder krishantering men det krävs att kunder är medvetna om att de behöver det eller ställer krav det.

Om uppkopplade enheter är ett problem, dvs. att de utgör en risk för potentiellt dataintrång eller för organisationen överlag
Generellt är folk medvetna men säkerhet prioriteras inte. De tar upp exempel om laptops (även om det inte är IoT) och generaliserar att förr var det fokus på brandväggar och liknande dataskydd. Datorer och mobiler är i fokus nu. Problematik när anställda tar hem sina enheter från jobbet och kopplar upp till sitt ADSL modem/wifi. Däremot finns det krypteringsskydd och liknande på anställdas dator. Problemet kommer när uppkopplade enheter ligger på samma WiFi exempelvis.

Respondenternas exempel på säkerhet gällande uppkopplade produkter
Ett annat exempel som tog upp var en utbildning på Mälardalens högskola. I utbildningen så lär sig eleverna att skapa uppkopplade produkter genom design och programmering men det ingår

inte någon säkerhetskurs. Mikko som varit i kontakt med dem anser att detta är ett problem. De lär sig designa dessa uppkopplade enheter/små datorer får inte lära sig säkerhetstänk och det blir fel prioriterat från början.

Ett till exempel på hur företag kan tänka gällande säkerhet och IoT produkter är hur IKEA gjorde gällande sina lampor med inbygg uppkoppling. Där är säkerhetstänket genomgående då IKEA tänkte att de tjänar på att göra säkra produkter, förlorar mer på om de måste kalla tillbaka alla produkter av en viss sort på grund av säkerhetsbrister. IKEA deltog i en konferens för hackare (Sec-T) och bad hackare att försöka hacka lampan genom att dela ut lampor gratis.

Exemplet om självstyrande bilar kom också upp under intervjun. Där finns problemet att säkerhetstänket fokuserar mer på själva säkerheten, t.ex. på tekniken och problematik gällande vad bilen ska köra på och likande. Kanske inte fokuserar lika mycket på informationssäkerheten, t.ex. att bilens mjukvara kan hackas.

Respondenterna tog också upp exempel som Ransomware attacker då företag fick sin information låst. Även exempel om att Tesla blev hackat.

Generella tankar om säkerhet

Christer: “Man har inte säkerhet - man gör säkerhet”. ”Säkerhet är ingenting man har – det är någonting man gör.”

De förklarar också att man inte får glömma att det oftast finns en ekonomisk bakgrund till säkerhet. Kommer företag tjäna på säkerhet eller är det bara en extra kostnad. Vissa företag kanske inte ser att det är värt med några extra kronor på säkerheten.

Respondenterna tror att IoT anses nu inte vara ett problem men kommer bli det i framtiden. Med tanke på att man designar och utvecklar IoT och i efterhand tänker på säkerhet. Enligt dem är detta fel ordning. Kommer bli problem i framtiden. Problematiskt när alla vill ha häftiga, uppkopplade prylar men bryr sig inte eller inte är medvetna om de säkerhetsrisker som finns.

Bilaga 3: Intervju med U-Blox 1

Intervju med Mats Andersson, Senor Director Technology	
Datum:	09-04-2018
Tid	09.03-10.03
Intervjuare	Emma Nilsson (E), Matilda Stading (M), Victoria Andersson (V)
Intervjuperson	Mats Andersson (M)

MA: Hej

V: Jag skickade tidigt imorse intervjufrågor, men i och med att du körde från Blekinge imorse är det helt förståeligt ifall du inte har sett dem än.

MA: Hehe, ja precis. Satt i bilen.

alla skrattar lite nervöst

Okej, men de finns på din mail om du vill kolla på dem nu under tiden.

Kort paus, tar upp datorerna

V: Sådär. Ja. Vi är i princip i mitten av våran uppsats, ville säga att vi är i början men vi har ju faktiskt kommit en bra bit.

E: Ja, det är vi ju.

V: Så, vi har valt att fokusera vår uppsats på att kolla på medvetenheten, eller rättare sagt olika företags medvetenhet gällande säkerhetsrisken i och med IoT. Så då har vi försökt att kolla upp företag som arbetar med IoT, med implementeringen av uppkopplade produkter, eller använder uppkopplade. Så det är lite olika. Så nu vill vi se hur ni ser på Internet of Things. Även om ni till skillnad från andra företag, fokuserar mer på utvecklingen av IoT produkter, så är det även extremt intressant för oss. Så det är därför vi hörde av oss till u-blox. Men det är i alla fall det vi har valt som ämne, och vårt fokus kommer att ligga på medvetenheten, the ‘awareness’, i och med att vi tycker att det är jätteviktigt inför framtiden

då IoT bara växer och växer. Och då skulle jag vilja börja med att be dig att berätta lite om vad u-blox är, och vad ni arbetar med.

MA: Jo. Vi tar ju fram moduler, komponenter för trådlös kommunikation i grunden och ett av de användningsområden för det är ju då bl.a. Internet of Things dvs att idén är att modulerna ska kunna byggas in i produkter för att kunna göra de trådlösa helt enkelt, alltså kunna kommunicera trådlöst med omgivningen. Då använder vi oss av tekniker som bluetooth, wireless LAN, en mängd olika radioteknikerdå för att kommunicera. Men samtidigt dessa produkter är ju typiskt små prylar, typ sensorer eller små apparater, där i många fall kundens applikationer också kommer ligga i samma pryl. Vi har då alltså en produkt som är en liten modul, med ett elektroniskt kretskort i princip, och i den så finns det en processor som där man både kan köra radiokommunikation plus kundens applikation, eller delar av kundens applikation. Det innebär då också att säkerheten börjar redan i vår produkt, och för det första så är det säkerheten över luften, så att säga, och det är ju vår specialitet liksom, men det räcker liksom inte, då med säkerheten över kundens applikation och hans egen dator, vilket vi också måste hjälpa kunden med. Och sen är det ju ännu mer än så, allting börjar ju egentligen med i produkten, och då måste man veta att det körs rätt mjukvara i den helt enkelt, och att den mjukvaran som körs i den produkten är den mjukvara som ska köras och då inte någonting annat. Där börjar liksom all säkerhet. Vet man inte det så vet man ju ingenting. Det är ju det vi kallar för Secure Boot, secure firmware, som är den mekanismen som… Vi då som företag, alltså jag har ju kämpat för det här länge för jag har tyckt att det är viktigt, och trott länge, men ‘the awareness’ hos kunderna har ju inte varit sådär jättestor, fram till för något år sen kanske. Så att, då har de ansett att “nej det är väl kanske inte så viktigt, vi vill ha massa andra funktioner i våra produkter och vi vill inte utveckla säkerhet, det finns andra grejer som är viktiga för våra kunder” (‘citerar’ en gammal kund) och kunderna har ju ännu inte riktigt upptäckt det (läs: säkerhet)det. Men det ändrades ju för kanske två år sen…

V: Skulle du säga att det har med IoT-trenden att göra, att deras efterfrågan på säkerhet ändrades?

MA: Det som hände då ju var att det dök ju upp ett antal fall utav riktigt problem. Jag vet inte om ni har hört talas om det men det finns ju en “Denial of Service”- attack som kom ifrån små prylar, alltså inbyggda datorer i produkter som då slog ut en massa sajter för kanske två år sen.

V: Vad kallade du det, sa du, den attacken?

MA: Denial of Service. Det är en sådan attack där någon skickar massa skräp till massa servers och på det viset slå ut servern, vilket var ju perfekt för då kunde man få ut den mjukvaran, den felaktiga mjukvaran, till många små prylar. Då är det helt plötsligt jättemånga enheter som kan skicka skräpdata, vilket gör ju att en denial of service attack blir väldigt effektiv. Förr har ju alltid attackerna skett från datorer, men det finns massa fler prylar än vad det finns datorer. Så om kan få ut den där farliga mjukvaran i dessa små prylarna som sitter i tvättmaskiner, och gud vet allt, så blir det ju en mycket större risk - eller alla i dina hemma-apparater typ som en router som där man får wifi, det var ju sådana

produkter i fallet där man lyckats få in den felaktiga mjukvaran, då blev det alltså en ännu större spridning på den attacken.

E: Så du menar att medvetenheten inte kom förrän… [att företagen faktiskt drabbades av konsekvensen att inte använda tillräckligt med säkerhet]?

MA: Nu är jag rätt generell, men vissa kunder var medvetna, men inte den stora massan. Så det var ju när något sådant hände, det har ju funnit fler liknande attacker… Det finns t.ex en video på Facebook, där man flög med en sådan är drönare som flög utanför en byggnad, som slog ut alla ljusen i byggnaden, och det var ju sådan där automatisk belysning som var styrd trådlöst, så hade någon hackat sig in i det och då kunnat släcka belysningen. Han gjorde ju ingenting 'farligt', men han hade ju kunnat göra något farligt med det. Så när drönare flög utanför fönstret på kontorsbyggnaden, så från ett fönster till ett annat så släcktes varje belysning. Så kunde han ju på verkligen påverka genom att släcka belysningen genom att tränga sig in i systemet och dess kärna, för att släcka.

V: Wow, läskigt och coolt samtidigt!

Gemensamt skratt

MA: Ja, det är ju något annat. Men det gjorde han ju genom en liten pryl som inte längre är en dator… Men inbyggda datorer har ju funnits länge, men små prylarna… Men som du sa tidigare, Internet of Things blev ju inte stort förrän de sista åren, så det är ju först nu som medvetenheten blivit större

V: Är det många kunder som ni har, som har återkommit till er med då problem som ni då fått lösa?

MA: Ja, det har ju varit ett par olika, de har ju varit något som heter 'crack', ett virus, som har varit innebärt en säkerhetslucka i bluetoothstandarden till exempel, som blev väldigt mycket press för ungefär ett halvår sedan. Då har många skrivit 'det är massa säkerhetsluckor i bluetoothstandarden' och egentligen var ju det ingen säkerhetslucka i standarden utan det var en säkerhetslucka i hur man implementerar standarden, men dock då fick vi bevisa att alla våra produkter inte hade den säkerhetsluckan. Då kom kunden till oss och sa att 'vi har läst i pressen, tidningarna och på internet att nu är bluetooth osäkert och vi använder ju bluetooth och ojojoj' men för de flesta var det inget problem, men vi var ändå tvungna att bevisa för alla våra kunder att det inte hände med våra produkter.

V: Ja men precis, för ni har ändå fokuserat på säkerhet sedan början, eller hur…?

MA: Ja, där kan man säga att vi har ett fokus på säkerhet nu, men vi hade det inte för tre år sedan.

V: Ja okej, och det är i och med att det ökar en efterfrågan från kunderna?

MA: Ja, jo, det kan man väl säga, plus att våran egen medvetenhet, vi har också försökt vara lite proaktiva, och lite varse om vår kunder. Så våra första produkter med Secure Boot t.ex. Har en sådan grundläggande mekanism som ser att det är rätt mjukvara i produkten. Den släppte vi i och med vår första produkt för ett och ett halvt år sen ungefär, och nu släpper vi ytterligare en produkt och det ska in i alla våra produkter (???) är tanken. Men det är så pass nytt för oss också. Det är därför vi håller på med det som kallad för End-to-End security, och det är i princip att om kunden ska skicka data från sin lilla pryl ut i molnet till en tjänst som de har på amazon eller någonstans, så vill man säkra hela förbindelsen från end to end så man har en säker länk hela vägen, och så att man inte bryter den länken någonstans i mitten som man ofta gör idag, utan då måste vi kunna lägga in - även de små prylarna vi gör - certifikat för att skydda hela vägen, ända ut till slutprodukten. Och det är ju också något som vi lägger in i våra produkter nu. Vi har alltid varit bra på säkerheten över luften, för standarderna - bluetoothstandarden till exempel - har ju inbyggd mekanism, till exempel när man parar telefonen till ett headset eller något sånt där så är det i princip att vi sätter upp en säkerhetsrelation mellan telefonen och headsetet så har det ju funnit en bluetooth alltid, eller likadant i wifi så om ni kopplar upp telefonen mot er accesspunkt hemma, eller router hemma, ja då så använder ni er av en VPA-nyckel som det heter då ju, då säkrar man ju själva länken - alltså radiolänken - men inte liksom det som går över radiolänken behöver ju inte vara säkert för det.

M: Aha, alltså det som skickas emellan?

MA: Säg att du har en pryl, som pratar med wifi till en router, och sen pratar den från routern via internet till en molntjänst på amazon eller något sånt där. Och med wifi så säkrar du då förbindelsen mellan prylen till routern, med den säkerheten som kommer inbyggt med wifit. Men sen från routern mot molntjänsten, och det är ju det som menas med end-to-end security, då vill man alltså säkra hela, även på den trådlösa säkerheten vill man nu lägga ytterligare en säkerhet som är från ‘ändpunkt till ändpunkt’, så nära källan av data till där datan ska hamna som möjligt. Och det är det som är end-to-end security, och förr var det ju inte relevant i sådana små prylar, med inbyggda system, sådana som liksom kan sitta inne i tvättmaskiner, nej det var ju inte relevant för det gick ju inte att göra då det var för stort. Det tar ju massa plats och kraft. Säkerhet kostar ju, det kostar liksom både minne och CPU-kraft, och det kostar, ja det finns ju massa kostnader som medföljer som kan omsättas till pengar. Större minne kostar ju pengar och man fick inte heller plats med det i små inbyggda produkter förr i tiden, nu måste vi helt enkelt göra plats.

M: Men är det så att det är enkelt att göra plats, om man kan säga så?

MA: Ja, det är ju egentligen är det ju kostnaden. Det är ju egentligen inget svårt att se till att man har tillräckligt med mycket minne i en sån här pryl egentligen, frågan är ju om kunden är villig att betala. De måste tycka att säkerhet är viktigt, så att de är beredda att betala de extra kronorna för sin pryl som ska ut flera miljoner stycken, jag menar ibland går det upp till 100 miljoner, och om man ska betala två kronor extra för varje pryl, ja då går vi upp i 200 miljoner extra för att ‘bara’ få den här säkerheten. Så de låter de bli säkerheten och tänker att ‘nej det är väl inte så farligt’ fram tills den dagen de åker dit. En sak ska man veta, de företaget som har en produkt som har en typ av säkerhetslucka - och det gäller även för våra

egna produkter - och om det kommer press, då blir den extrem och det blir snabbt väldigt mycket skriverier i tidningar och datorpress, och det är ju inget bra.

V: Hur hanterar ni det, ifall det skulle hända? Om det kanske redan har hänt?

MA: Vi har inte direkt råkat ut för det ännu, men bara indirekt då en kund som drabbats. Men vi har ju folk som håller på att bygga upp en organisation runt företaget som tar hand om sådana saker. Om vi t.ex. Säger att vår produkt är säker, och det sen visar sig att vi råkat göra något fel som inte är säkert, då måste vi ju kunna hantera den situationen som inträffar då och det är inte helt enkelt. Marknadsmässigt och så.

V: Vad skulle ni säga att era kunder har prioriterat - utöver säkerheten - i och med att säkerheten har dykt upp nu på sistone? Vad har varit viktigare, har det då varit utvecklingen för särskilda funktioner istället?

M: Ja, det har ju varit mer funktioner. Mer allmänt andra, dels det som prylarna egentligen gör. Säkerhet är ju inte det prylarna 'gör'. Till exemple en kund som gör en tvättmaskin som man kopplar upp mot internet, de vill ju kunna skicka iväg tvättmaskinsinformation till internet, och bryr sig ju inte om säkerhet i grunden. För de är ju säkerhet något de måste ha. De har ju alltid satsat på funktioner först, och många har missat säkerheten. Kopplar upp sin pryl mot internet, och sen tänkte de inte på… Eller jo, de kanske tänkte på det, men slarvade med det. Fram tills den dagen de åker dit då ju. Det som jag berättade om det här med belysningen (och drönaren), det var ju Philips och de är ju en av världens störts belysningsföretag som råkade ut för det där. Det var ju inte så roligt för Philips då, att se de videona där en drönare slår av hela deras belysning.

V: Vilken snackis!

MA: Ja, det blev det ju! Det blev ju världens hallå om det.

V: Skulle du säga att det är skillnad på större och små företag när det kommer till säkerhet och dess prioriteringar?

MA: Ja, det skulle jag kunna säga generellt. Större företag är ju oftast med medvetna än små företag, skulle jag påstå. För de finns ofta i deras organisation att någon har hand om det. Sen är det ju inte säkert att tar tag i det ändå, men.. Men säg att du har en bra affärsidé, och du har ett startup-bolag, där du kommer på den här smarta, uppkopplade blomkrukan eller vad det nu kan vara, så tänker du inte ofta på säkerheten utan du tänker mer på att få ut produkten. Men däremot, företag som Philips, Siemens, de tänker ju säkert mer på det. Definitivt nu i alla fall.

M: Ja, de fick ju säkert en tankeställare!

MA: De fick absolut en tankeställare!

V: De har ju även resurserna, så man tänker ju att de absolut borde prioritera säkerheten! Men nä.

M: Det är ju en utmaning för oss som företag. I och med att vi tillverkar komponenter för Internet of Things, vi gör ju inte själva produkten. Det är våra kunder som gör produkten. Så om vi kan förse våra produkter med en säkring av internet of things, alltså funktioner, då får ju kunderna det på köpet så att säga. Köper någon då vår produkter och bygger in det i sin, köper dem då vår 'Nina V1' som är en wi-fi modul som har en secure boot inbyggt, de får de ju secure boot med i sin produkt. Även det lilla företaget som tillverkar blomkrukan, så kan startupen få en secure boot från oss.

V: Så man hade ju kunnat tycka, att företag som ni som utvecklar de här produkter, att det är de som gör säkerheten? Att det är de som löser problemet åt nästa kund?

M: Ja, men det gör vi ju. Det är det vi försöker göra. Vi försöker hjälpa, genom att ha de funktioner i våra produkter som gör det lättare för våra kunder som då är slutproduktutvecklar, genom att göra de säkrare. Det har blivit nästan en affärsidé för u-blox nu att vi ska ha säkerhet som en topprioritering. Om man går in på vår hemsida ser man att det finns ett helt kapitel om säkerhet. Det är viktigt för oss att vi visar att vi satsar på professionella kunder som bryr sig, säkerhet är en sådan viktig faktor.

M: Hur är det med era konkurrenter? Det här kanske blir en konkurrensfördel för er?

MA: Vi försöker få det till det ju. Andra har ju hänt på på trenden nu också. Det är många som satsar på säkerheten just nu ju. Men absolut, vi vill ju ha det som en konkurrensfördel.

V: Jag tänkte kolla lite på vilka krav som kunden ställer gällande säkerheten? Men då är det att ni gör det åt dem på ett sätt?

MA: Ja, fast det är ju både och. Det finns ju de kunde som genom att köpa våra produkter så blir de säkra utan att tänka mer på de och sen finns det ju de andra kunder som i princip letar efter att leverera som kan leverera prylar som innehåller de rätta funktionerna för säkerhet. Då är ju vi den leverantören. Och vi vill ju framförallt vara den leverantören. Köper man vår pryl och bygger in i sin produkt så ska de få säkerhet, på den nivån som kunden önskar. Det är ju också det att säkerhet ligger på olika nivåer, och det finns ju olika kostnader. Ju mer bra eller tillförlitlig säkerhet, desto högre är kostnaden. Det finns olika graderingar kan man säga.

V: Skulle ni säga att det är en av topprioriteringarna i nuläget? Tillsammans med de rätta funktionerna då.

MA: En av topprioriteringarna absolut.

V: Hur såg det ut innan?

MA: Går man tillbaka tre år så var det absolut inte det. Det är ju ganska nytt.

V: Om vi inte har fler frågor på ämnet, så skulle vi vilja veta om ni på u-blox använder er av uppkopplade produkter, på ert kontor?

E: Förutom standardenheter som datorer, mobil etc.

MA: Vi gör ju inte det själva. Det är främst våra kunder. Det är klart att vi har demoprodukter och så och de måste vi ju kunna bevisa att de är säkra.

V: Vi tänker ju att ni besitter ju ändå på information som ni vill hålla inom företaget?

MA: Vi har ju inte så eget uppkopplat själv, eller slutprodukter. Utan det är ju kunderna. Men å andra sidan så är det ju tusentals kunder som har våra produkter i sina. Mycket av det vi köper har vi ju det. Till exempel, om man köper en bil idag så är det en stor sannolikhet att det sitter en bluetoothprodukt i den. Då är det ju bra att veta att de är säkra då ju.

M: Är det sådana kunder som ni har?

MA: Ja, till exempel! Bilindustrin är en viktig kund. Biltillverkare är en typisk en kund. Även tillverkarna av mediciniska apparater, det säkerheten är jätteviktig. Industriell teknik överlag, där är säkerheten också viktig. Det är kunder som har produkter som har typiska krav för säkerhet. Ett bolag som gör medicinsa enheter t.ex en infusionspump, ett sådant företag är ju väldigt medvetet om säkerheten och vill ju verkligen veta att ingen hackar in. Det är det ju frågan om att folk kan dö i de fallen.

M: Och nu med bilar också… Nu när det är aktuellt med självkörande bilar.

MA: Ja absolut, det är ju ett av våra arbetsområden. Det är ju säkerheten, och sen finns det ju ‘safety’. Det är ju inte bara säkerhet, utan man mer dubbelkollar att allting är rätt, att det handlar om att man skyddar liv. Det blir ju en dimension till av säkerheten. Utan säkerhet i botten. Har man t.ex inte Secure Boot i en bil, och man kan byta mjukvaran så kvittar ju allt. Det handlar ju om grundläggande säkerhet. Secure Boot är ju till för att man ska veta vilka mjukvara som körs och att den är rätt. När det kommer till självkörande bilar är det ju både säkerhet och ‘safety’ som måste gälla.

V: Angående framtiden, vad tror du är nästa steg inom IoT? Man förutspår att det kommer finnas miljontals - rättare sagt miljardtals - med prylar som kommer vara uppkopplade? Hur ser u-blox på detta? I och med att ni har ändå en stor del av det, skulle jag vilja säga.

MA: Därför det är det viktigt att vi kan förse våra kunder med säkerheten. Vi tror ju att det här kommer bli jättestort, att det här bara är början på Internet of Things eran. Det kommer bara bli mer och mer. Tänk på det att förr var ju uppkopplad krin

MA: Därför det är det viktigt att vi kan förse våra kunder med säkerheten. Vi tror ju att det här kommer bli jättestort, att det här bara är början på Internet of Things eran. Det kommer bara bli mer och mer. Tänk på det att förr var man mer uppkopplad till människan, och tänk då att vi är runt 10 miljarder människor och om varje människa har två stycken till exempel

mobiltelefon och dator. Ja, är vi uppe i 20 miljarder prylar.. Men nu med Internet of Things, tänk då alla prylar som finns i världen... Det är ju 50, kanske 100 miljarder. Det blir en helt annan dimension på både mängden prylar samt säkerhetsproblemen. Då kan prylarna göra en mycket större skada på uppkopplade program eller andra uppkopplade prylar på datorer.

M: Jag tänker på att eftersom ni har då 'början' på produkten, kan man kanske säga, och den är säker då man inte kan byta ut mjukvaran. Hur blir det då i slutskedet? Finns det någon annan slags säkerhetsrisk på vägen, som du ser?

MA: Det kan ju vara så att i vissa fall så har kunden har en egen processor eller dator i sin produkt, då är det ju klart den behöver ju också säkring, och då försöker vi hjälpa dem med det. Så end-to-end security till exempel skulle vi kunna 'skruva ihop' och hjälpa dem. Vi får ju se till att hjälpa våran produkt genom att hjälpa deras produkt. Vi gör ju sådana typer av tjänster. Till exempel, en MCU eller en processor som pratar med vår pryl, då har vi ju ett interface där i mellan och det är ju också en känslig punkt för säkerhetsmetodiken (?) och då får vi hjälpa till och se till att det är säkert, så att det inte ska bli möjligt för någon annan att ta sig in mellan där (mellan processorn och prylen). Vi försöker ju hjälpa kunderna att göra deras produkter säkra, det är ju vår ambition. Men sen är det mycket mer vi gör idag. Ett problem är ju också att metoderna för att hacka sig in i system blir mer och mer sofistikerade. Därför måste säkerheten förbättras hela tiden. Bara en sådan sak att om man har krypterat, så gör man det med nycklar, och nycklar med viss bitlängd - det finns längd -, och har man en tillräckligt långa nycklar så kan man inte idag bryta krypteringen, men vi vet ju att metoderna blir ju snabbare till slut och då kan de räkna ut ett sätt för att bryta krypteringen. Det rör ju sig framåt hela tiden. Vi försöker ha en framförhållning, så vi håller en viss 1028 bitars krypteringsnyckellängd, så vi klarar ju oss efter ett beräknat 30-40 år. Men sen vet vi att det kommer snabba datorer som kan byta den typen av kryptering.

E: Jag tänkte precis fråga det. Hur ställer ni er till att själva hackersen, eller datorer, blir mer och mer duktiga på att hacka? För det tvingar ju säkerheten att alltid hållas uppdaterad.

MA: Ja, det är ju det... Man måste ju alltid ligga lite före. Till exempel idag räcker en 512 bitars nyckellängd för det finns ingen dator som är kraftfull nog att bryta den, så då kan man använda 1028 bara för att man vill se till at det är framtidssäkert. Man måste hela tiden tänka på att ligga före. Sen vet man ju samtidigt att det finns ju många tittat och försökt hacka sig in men debatten om detta är ju större är någonsin. Och även de typer av hackerattacker, det kan ju mycket väl gå genom apparater. För ett antal år sen i ett iranskt kärnkraftverk, det är ju inte så himla kul att man kan hacka sig in och styra ett helt kärnkraftverk..

E: Sådana typer av händelser måste ju verkligen ligga på prioriteringslistan när det kommer till säkerhet!

MA: Ja, absolut. Så var det ju säkert också, eller ja det trodde de! Men så kom det några som var smartare, och det är därför många IT-företag anställer hackers för att hjälpa.. Vi har ju även anlitat företag, alltså konsultföretag, som är hackers som kan testa produkterna. Då säger man ingenting till dem, utan man ger dem produkten och låter de testa sig fram och se om de kan hacka sig in i den.

E: Och ni gjorde också det sa ni?

MA: Ja, precis. Inte här i Malmö direkt, men runt om i England, som gjorde exakt det där. Så det är ju före-detta hackers som har startat företag kring det här, att hjälpa företag att se om deras produkter har 'hål' som man hade kunnat hacka sig in i. Det är ju rätt intressant.

M: Viktigt med! Ser ni att det är ni företag som tar den här frågan framåt? Att det är ni som ser till att det är säkert, då ibland kunderna inte ställer krav.

MA: Ja, jo, men det håller på att ändras! Många kunder kräver idag att och även vi som konsumenter kommer att kräva det här nu. Det som har hänt nu... Man ser ju själv...

M: Hur ser det ut med myndigheter? Finns det några krav från myndigheter på er?

MA: Det kan det ju finnas. Ni nämnde ju själva det här med självstyrande bilar, eller medicinskt teknikt. Till exempel i USA så finns det något som heter Pheebs Compliance (googla om detta stämmer). Det är en standard som satts från den amerikanska militären, där de har sagt att att om man ska använda sig av olika balker(?) så måste man följa pheebs. Det började ju i militären, och sen har det gått in i olika regler nu då, medicinsk teknik då till exempel. Det började dyka upp standarder också, då EU-standarder eller amerikanska standarder mot säkerhet, men det har ju inte funnit så mycket tidigare heller.

E: Är de tillräckligt höga, eller är de rätt så låga?

MA: Nja, det är ju rätt varierande, men det nog inte tillräckligt högt. De är ju är rätt uppskärpta (?). Men om man vill hålla den uppkopplade världen uppkopplad, det finns ju en gräns på vad man är beredd på att betala. Både för mycket. Kostar säkerheten för mycket kanske det inte blir en produkt ens, för ingen är beredd att betala för den. Säg att du köper en uppkopplad lampa och hur mycket är du beredd att betala extra för den för att du ska veta att någon om 15 år kan hacka sig in.

E: Nä, just i det tillfället låter ju inte det så lockande.

MA: Tills den dagen plötsligt hela staden släcks.

M: Och det är det jag tänker på det här med myndigheter, om det nu ska finnas en ‘smart stad’, hur mycket är en stad/kommun villiga att betala för lite extra säkerhet på produkter som är uppkopplade t.ex papperskorgar.

MA: Jag tror att det är finns vissa områden där medvetenheten är ganska låg. Vi är ju med i lite sådana projekt i t.ex Lund och Malmö där man fått in smart city projekt där man ska testa teknik, och ja det är klart man pratar om säkerhet men det är inte så att det ligger högst på agendan utan det är ju mest att funktionerna ska funka som de ska t.ex soptunnan eller vad det nu kan vara. Man kan ju fråga sig i just det fallet, om någon hackar sig in i soptunnan, är det så viktigt? Då kanske man drar ner på säkerheten för att man inte tycker att det är lika

viktigt. Jag menar, hackar man sjukhuset så är det ju annorlunda då är ju produkterna hjärt- och lugnmaskiner.

M: Frågan är ju då, om i framtiden i sådana städer att om man kan hacka en grej, så kan man hacka resten och till slut så kan man stänga ner en hel stad.

MA: I sådana DDOS-attacker, det är ju mest att man skräpar ner "luften" eller rättare sagt nätverken, så mycket att systemet stannar skulle man ju kunna.. låt oss säga att man skulle ha alla soptunnor uppkopplade eller att de sitter i samma nätverk, så om man skulle hacka sig in i alla soptunnor i Malmö då är det många som kan skicka 'skräp via luften', en så att säga DDOS-attack.

E: Då är frågan om det är värt att ha en 'smart city'?

MA: Ja, då får man ju räkna in säkerhet som en komponent i det hela ju..

E: Dubai vet jag ska ha ett fritt internet över hela staden snart, det blir första staden som provar det på riktigt. Ja, det låter ju bra men frågan är ju hur det kommer gå..

MA: Det är ju rätt lätt om man t.ex har stadsnät som staden betalar för att kunna att kunna surfa, man kanske inte kan använda det nätet för att använda just det nätet för att koppla upp soptunnorna utan man måste använda ett annat nät, en annan teknik, parallellt.

E: Ett annat nät, för just sjukhus osv..

MA: Ja, just sjukhus de har ju ofta de dilemmat att de försöker hålla isär det som är livsupphållande från det som bara används [...övriga saker]. Jag menar, om du är på sjukhus idag så tillåter dem att du kopplar upp dig till deras nät. Innan tillät de inte det, men det får man på sjukhus nu. De har ju släppt på det till en viss mån, och då gäller det att de verkligen tänker på att de håller isär på det som de har internt och på det deras patienter använder.

M: Frågan är ju om de är medvetna då..

MA: Inte alltid tillräckligt mycket. Men det har blivit mer. För det finns ju ofta säkerhetsanställda på de den typen av institutioner som sjukhus, kommuner, osv. Där är det folk som har säkerhet som ansvar. Då tänker folk ofta när de hör 'datasäkerhet' att det är personsäkerhet men tänker ofta inte på själva prylarna.

E, M, V: Nä, precis!

MA: Det kan ju ofta vara ett problem, att det bara är duktiga på att skydda personlig integritet. Då glömmer man bort resten.

M: Med prylarna kan man ju få tag på den här personliga informationen på något sätt.

MA: Ett bra exempel är ju uppkopplade medicinska apparater som hjärtövervakningsutrustning t.ex och så knappar du in ditt personnummer, och den informationen där kan ju vara intressant. Då vet man en person som är hjärtsjuk som har det här personnumret, det är ju personlig information. Det är ju den uppkopplade prylen då som innehåller informationen som är personlig. Det är ju likadant i det uppkopplade hemmet, där man har tvättmaskiner, lampor, allt möjligt, där finns informationen som är uppkopplad som säger att man använder tvättmaskinen två gånger om dagen eller två gånger i veckan, det är ju sådan information som går att använda sig av. Det är ju också personlig information.

M: Det är ju också många företag, typ tvättmaskinsföretag som ser det som viktig information.

MA: Ja, då kan de ju skicka ut meddelanden, typ riktad reklam, exempel att 'nu har tvättmaskinen körts 2000 gånger och nu är det dags för service!'

M: På det sättet är det ju företagen som använder informationen från sina egna produkter.

MA: Ja, det gäller ju att hålla isär det. Vem vet att det är bara är ett 'vanligt' företag? Kolla bara på det där med Facebook nu, då är det ju information som de hade som någon annan fick tag i.

M: Ja, det är ju väldigt lätt för företag att sälja sådan data eller då själva hacka den.

MA: Ja, det var ju också för studenterna i Lund… Jag hörde det på radion i bilen att det var någon form av registrering av studenter som var helt öppen, alla personnummer och adresser för alla studenter i Lund var öppna ett antal dagar.

E: Kanske, Ladok? I och med att de håller på att pilla med det.

V: Ja, hela vårt betygssystem ligger nere just nu.

MA: Aha! Ja, men det var någon form av information som var helt öppen.

M: Det har ju blivit väldigt mycket medvetenhet genom GDPR också, det har ju kommit upp nu, och det handlar ju om privacy och personlig information. Men jag ser det som kanske en start på detta, från EUs håll, ändå, för nu börjar folk tänka på det mer.

MA: Jag tror det kommer komma mer regler, lagar och standarder som man måste följa som har med säkerhet att göra. Det är ju bara början, från EU då. För oss kommer det bli lite besvärligt, det är helt klart. Men det kommer säkert komma mer. För det finns ju krav.. Kunderna kommer ju att kräva på att man uppfyller en viss, specifik standard. Om kunden kan peka på en standard som någon institution har tagit fram, är det bra för dem att garantera. De kanske inte behöver allt i just den standard, men så länge de uppfyller den så kan kunden se att det är säkert. Som det här med den amerikanska militären. Det är ju garanti på att produkten är säker med en sådan standard.

M: Frågan är ju om de är tillräckligt med i tiden, jag menar företag kanske redan har superbra säkerhet men kanske på en annan standard.

E: Sen kan det ju vara så att man är fullt säker idag, men imorgon så kommer något snille på en bra ny ide..

MA: Men en sak ska ni veta om säkerhet! Den dagen vi har kvantdatorer, eller datorer som är kvantmekaniska. Det kanske känns långt borta men tro mig, skulle någon uppfinna en sådan dator som går miljoner gånger snabbare, då kan man ju bara glömma alla andra krypteringsmetoder för då kommer de kunna hacka allt. De har de en sådan datorberäkningskraft, där man kan iterera sig fram till lösningen på den här krypteringsalgoritmen.
V: Jag undrar om man redan förbereder sig för det? Ifall det skulle kunna hända relativt snart?

MA: Skulle vi kryptera våran information, eller våra radiolänkar till exempel, med kvantdatorer så hade vi varit tvungna att en kvantdator i prylen också. Men så gör man ju inte, man säger att med den datorutvecklingen vi har idag, så kommer vi klara oss i kanske 50 år. Skulle något sådant steg tas att sådan teknik finns, då får man tänka om med säkerheten. De nya tekniker till exempel blockchain, som man använder för säkerheten, det är en sorts nät, det är ju mycket möjligt att det kan vara framtiden, då är det mer ett system som ger säkerheten.

V: Är det någon som ni arbetar med?

MA: Nja, det har tittat på det, men vi har inte.. .Vi är med mer i bakgrunden. Det är mycket på konferenser, det här med blockchain och säkerhet kring det. Det börjar dyka upp!

M: Skulle ni kunna ha det i era produkter?

MA: Det knepiga är det att det är bara de produkter som är uppkopplade. Till exempel det här med radiolänk från A till B, det i sig har ju inte kontakt till nätet, och blockchain bygger på att man har kontakt med nätet för att kunna använda det. Man verifierar kontakt genom en ‘kedja’ som består utav blocks, och då kan det bli svårt.. För våra uppkopplade produkter skulle det kunna bli väldigt intressant. När du idag verifierar dig mot din bank, så gör du det med en dosa eller något i den stilen istället för att använda en blockchainmekanism. De här dosorna använder ju en slags kryptering. De innehåller en viss nyckellängd och då litar man ju på den, att den inte går att hackas. Jo, visst det går, men det skulle ta 50 år för en dator. Det tycker man är okej idag.

M: Men sen så kommer bankID, och sen kommer något annat ID.

MA: BankID är ju att man använder certifikat som har en viss nyckellängd också, så då har man bestämt att det är okej om det är 1024 nyckellängd. Det skulle ta lång tid, men det är okej.

E: Det är ju helt otroligt vilken baktanke det ligger, vi bara laddar ner appen och sen använder vi den…

MA: Ja, det är ju mycket tanke bakom.
E: Men visst blev det ifrågasatt, det där med bankID?

MA: Det var mer med hanteringen av det, inte själva algoritmen.

E: För det var ju viktigt under en period att man uppdaterade den, för extra säkerheten.

MA: Jag tror inte de har ändrat något med själva krypteringsalgoritmen, utan mer hur programmet är uppbyggt. På något sätt måste man visa den här nyckeln i klartext, men folk missar ju sådant. Det är ju människor som programmerar. På en bank så sitter där en programmerare som kan tänka smart, men som sitter på en nyckel. Det finns ju alltid folk som är bovar också…

E, V, M: Ja, precis!

MA: Det är ju faktiskt en människa som gör det.

E: Det har jag läst rätt mycket om, att det finns en hel del anställda som är villiga att sälja information till ett visst pris.

MA: Jag kan absolut tänka mig att det händer, på banker är det viktigt framförallt. Bankerna är redo att betala mycket för att de ska hålla tyst om en sådan grej, för det skulle bli en himla stor grej.

M: Ja, de har väl resurserna..

MA: Men det är samma sak i prylar. Det är ju programmerare som gör det, sen måste systemen.. I vårt fall, vi håller på att bygga upp en organisation kring det här, att vi ska ha personer som verifierar det vi har gjort i våra produkter. Det är ju en del av säkerheten också, inte bara att man vet hur man ska programmera, för det kan man ju läsa sig till i böckerna, utan man ska till att det är gjort på rätt sätt också.

E: Ja, och att ingen har missat någonting heller.

MA: Nä, precis. Där håller vi på med att bygga upp en organisation kring det här, att vi ska ha några experter som oberoende tittar på det vi har gjort.

V: Hur mycket ‘outsourcar’ ni för att säkerhetsställa att era produkter är som de ska vara innan de skickas till försäljning?

MA: Vi använder oss utav tredjepartsexperter, typ konsulter och liknande. Tänk på det här med secure boot, det innebär att när vi producerar våra produkter i fabriken, då ska den här mjukvaran laddas ner på ett säkert sätt i produkten. Det betyder att det finns en infrastruktur

bakom, i fabriken, med hanteringen av nycklar där. De hemliga nycklarna finns ju någonstans. När du ska kryptera din mjukvara när man gör Secure Boot, då gör man det med en nyckel, och den nyckeln den måste ju hanteras på ett absolut säkert sätt. Det är ju en hel process runt hur man hanterar hela den nyckeln, och hur man gör det på ett säkert sätt. Det ska ju vara smidigt för utvecklarna om de ska hantera den, så då byggde vi upp en rutin kring det där. Och att vi gjorde det på rätt sätt, så att inte den nyckeln aldrig går ute på 'farliga ställen'. För att säkerhetsställa det så använder vi oss av ett tredjepartsföretag som kom in utifrån som är experter på den typ av säkerhet, och tittade på hur vi gjorde för att bedöma att vi gjorde det på rätt sätt. Det var ju just för att få en garanti på att vi gör det på ett sätt … De kunde också tala om om de svaga punkter som finns, för det finns ju svaga punkter i allting. Det finns ju inte 100% säkert, det finns ju någon form av lucka någonstans och det gäller att minimerar och gör de svåra att komma åt. Då kunde de peka på att "här är de svaga punkterna, det här ska ni tänka på för att göra det extra tätt". För det är alltid någonstans, någon människa.. Om vi låser in alla nycklar, alla de privata nycklar som de heter, i ett gömt rum i England någonstans, så är det ju NÅGON som har nyckel till det rummet, NÅGON kan ju ta sig in. Då finns det en process kring det där. Det måste finnas två personer som i en viss ordning, öppnar det systemet. Det måste finnas någon chef på en viss nivå osv. I mitt fall, så ibland får jag ett meddelande från utvecklare, då jag är en av de som måste godkänna, och då får man ett meddelande som säger att jag måste gå in och godkänna att han använder den nyckeln, den och den nyckeln, och då ser jag att någon försöker få tag på den. Det är en hel process, som är rätt tung för företaget, den kostar.

E: Men annars, så kostar det ju…

MA: Ja, det finns ju en kostnad på andra hållet, om nyckeln skulle komma ut. Säg att vi har en produkt som tar ut två miljoner exemplar, så kommer den privata nyckeln ut. Ja, då är de två miljonerna i princip….

V: Ja.. Jag tycker att vi har fått väldigt bra svar! Vi är supertacksamma. Skulle ni säga att det finns en anledning till varför ni inte använder er av uppkopplade produkter på u-blox? Tror ni att ni kommer göra det i framtiden i och med att bli större..

MA: Alltså, vi lever ju på det vi gör.

Alla skrattar *

MA: Men ja, givetvis, vi måste ju hänga med på det här. Vi måste ju inse att för att göra uppkopplade produkter så måste det vara säkert. Så därför har vi satt det som ett av våra huvudområden, då vi vet att det kravet kommer att öka.

V: Undrar om det kommer bli ett slags val - att välja att har sitt företag uppkopplat eller inte pga säkerhetsrisken?

MA: Det finns ju de som är paranoida som säger att "vi kommer aldrig koppla upp oss", men medicinsk teknik är ett bra exempel. Livsupphållande maskiner, att styra en infussionspump i en medicin till blodet på folk. för att De är ju elektroniskt styrda. Det har varit väldigt

intressant för företag, även för läkare, att övervaka och styra den pumpen centralt genom trådlös förbindelse till exempel, att övervaka ja, men att styra den kommer bli väldigt svårt för dem. Även om det är 100 % säkert. Men vi kommer ju att använda självkörande bilar, det hände en olycka för ett par veckor sen där det mycket skriver om uber, men jag tror ändå att det där med förarlösa bilar, det kommer! Det kan ta några år men. Då är det helt plötsligt bilar som kör omkring utan att det är någon människa i.

M: Det finns ju redan tåg, tunnelbanor osv!

MA: Å andra sida, kan man vända på det och säga att vi människor är ju inte ofelbara precis. Så bakom ratten att fråga vem som är värst. I en självkörande bil finns det ingen som somnar, ingen som surfar mobilen.

M: Men det måste ju finnas en människa som gör dessa valen, som har programmerat det.

MA: Exakt, exakt. Ja, det kommer bli intressant. Om självkörande bilen står inför valet att köra på en femåring eller köra på en buss med pensioner, vilket val tar den då? Etiska problem blir ju något helt annat.

Paus. Kollega kommer in för underskrift av intervjuperson.

MA: Ja, det finns ju i många olika prylar etiskt beslut som måste tas.

M: Typ som vadå?

MA: Den informationen som samlas in om människor, jag menar, folk som kopplar in prylar, som gör sitt hem uppkopplat, de är inte själva medvetna om den information som man ger ut. Så det betyder ju att de företag måste göra en etiskt bedömning. Och sen det här också med GDPR.. T.ex. om det kommer någon från en bank som säger att reglerna kommer att ändras, som beror på GDPR, skulle ni läsa den texten då?

V, M, E: Njaee…

MA: Väldigt få gör ju det. Så kommer det en jättelång text, och i slutet så trycker man OK. Då har ni skrivit på då att ni godkänner att ni tar personuppgifter osv.

E: Ja, det är ju likadant när man laddar ner program så klickar man bara i boxen.

MA: Ja, de där boxarna.. Appar i telefonen är ett bra exempel, positionstjänster och all det där, hur många vet vad de klickar i där? Inte många!

E: Det har ju också lite med medvetenheten att göra, många bryr sig inte…

V: Ja, men det ligger ju på olika nivåer? Man har privatpersoner, man har företag, men jag kan tänka miga att det är viktigast med medvetenheten bland företagen då det är de som har makten, sen har de ju också med utbildningen att göra men det är ju en annan grej.

MA: Ja, men till exempel så har jag ett väldigt uppkopplat hem, man får ju leva som man lär. Där vet man ju liksom att när man kopplar upp sin belysning och allt det där mot servern då på Philips för informationen, då när man öppnar de lådorna så finns det papper där det.. Kollar man nogrannt så har man ju godkännt. Men om man kollar igenom vad man faktiskt godkänt, så skulle det säkert vara många som inte skulle ha godkänt.

E: Så intressant!

M: Ah, och då får alla företag också ett ansvar: "Ska vi utnyttja detta?"

MA: Ja, det finns ju absolut ett ansvar från företag också och då kommer vi in på etik och moral helt plötsligt, men det är ju det handlar om.. Men tänk på att vi precis börjat med uppkopplade prylar, men man tror att 10-15 år från nu så kommer alla nya hem vara uppkopplade, och då verkligen allt

M: Ja, och då har man ju skrivit på att man köpt ett hus och då får man "allt" på köpet.

MA: Personlig integritet är ju ofta den delen av säkerhet som folk ofta tänker mest på, och allt det andra som att deras prylar skulle kunna användas för att förstöra för andra, det tänker folk inte ofta på. Men det är ju faktiskt så också, om man kopplar in routern i sitt hem, som inte är säker så kan i princip fördärva för dina grannar. För i princip så sitter ni på samma nät, och den aspekten tänker man ofta inte på.

V: Man kanske bara måste acceptera det om man väljer att leva ett uppkopplat liv, i en uppkopplad stad att det finns en risk…

M: Men bara det med Dubai t.ex då tänker man kanske bara "Åh, gratis wi-fi och nu kopplar jag upp mina prylar på det här, superbra"...

MA: Men det här med att använda publikt wi-fi, det är sådant end-to-end security, om man kan säkra din förbindelse till end-to-end ändå trots att man kör på publikt nät, det som gäller är bara att inte göra informationen tillgänglig för andra, det är det som är end-to-end security. Då har man säkrat punkt till punkt, även om man kör på publikt nät. Det är ju det man gör hela tiden med, du kör ju på internet. De har de end-to-end security, när du använder dina dosa och autentiserar dig, då får du sådan https, då har du gjort en krypterad förbindelse. Samma sak kan du ju göra med din uppkopplade pryl, och då kan du använda ett publikt nät. Det enda problemet kan möjligtvis vara att det publika nätet är osäkert, då kan man tappa förbindelsen. I vissa hem har man kommit fram till att om man tappar förbindelsen så går det inte att släcka lampan. Faktum är att många har sådana uppkopplade hemautomationssystem som bygger på att man har en kontinuerlig kontakt med servern, så då kan man inte släcka lamporna när inte nätet fungerar, vilket ju är lite konstigt!

Alla skrattar
V: Och ju mer man tänker på det så är det ju så himla stort ämne, man kan gå in på så många nivåer så det är ja…

M: Men det känns som att som du säger, att det finns två olika problem att det både handlar om personlig integritet, och säkerhet gällande attacker osv

MA: Ja, och attacker kan ju både vara att de attackerar dig, och att dina prylar används för att attackera andra. Två sorters attacker.

M: Ja, men man kan ju kanske bygga ner det… Jag ser uppsatsen lite framför mig *hehe*...

MA: Teoretiskt sätt skulle man kunna tänka sig att om man tar ett belysningssystem om man tar Philips som exempel, eller IKEA med sina lampor och det, tänk då om det systemet skulle vara öppet så att om någon skulle komma på en algoritm som skulle kunna styra alla IKEAs lampor samtidigt. Det skulle ju kunna skapa ganska jobbiga scenarion för många, att lamporna börjar blinka lite hur som helst. Även om det inte kanske är farligt, så blir det ju väldigt jobbigt.

M: Ja, men tänk en ugn? Då blir det ju mer farligt.

MA: Men tänk även det här med lamporna, om det inte går att tända lampor…

V: Ja, då kommer det ju inte gå att styra sin egna tillvaro längre.

V: Vilket samhälle alltså!

MA: Ja, det får vi ju lösa med säkerhet!

Skrattar
V: U-blox fix!

M: Vad bra!

E: Tack så jättemycket!

V,M: Ja, verkligen!

M: Nu får vi hoppas att inspelningen fungerar…

Bilaga 4: Intervju U-Blox 2

Transkribering 3

Intervju med Martin Jerling, Senior Engineer	
Datum:	05-04-2018
Tid	10.11-10.35
Intervjuare	Emma Nilsson (E), Matilda Stading (M), Victoria Andersson (V)
Intervjuperson	Martin Jerlin (MJ)

Transkribering av den andra intervjun på u-Blox, Måndag 9 april. På u-Blox kontor i Malmö i ett labbrum då intervjupersonen arbetade samtidigt. Intervjun var spontant påkommen eftersom intervjupersonen bestämde sig för att prata med oss samma dag. Intervjun blev därför ganska

V: Vad är det du arbetar med på u-blox?

MJ: Gällande säkerhet håller jag på med infrastruktur och våra produktreleaser.

M: .. och vad mer specifikt gör du då?

MJ: Ser till att vi har våra nycklar korrekt för våra olika produkter och att de releaser vi gör ute i fabriker att vi har gått igenom en säkerhetskontroll på dem samt se till att nycklar kommer distribueras till de ställen som ska ha dem. Det är väl egentligen det enklaste förklaringen.

V: vilka krav har beställaren gällande säkerhet? Du behöver inte ge alla detaljer.

MJ: eh, det är under upparbetning, detta är som vi har just nu, så följer vi den branschpraxis, kan man säga, standarder utsedda för dem. Så atte eh, det blir lite efterhand som det kommer. Vi för en diskussionen med lite olika parter inom u-Blox hur vi ska göra.

V: ehm, skulle du säga att vissa av era kunder inte har så bra koll på säkerheten?

MJ: det skulle jag nog säga. De vet om att det är viktigt men det är nog svårt för som att definiera exakt vad de behöver för något. För säkerhet är så pass brett område så allt som oftast följer

deras egen bransch vissa krav till exempel om det är medical och patientjournaler eller så vill man bara ha linan säker så man inte har nått problem då.
V: okej nu ska vi se.

(intervjupersonens kollega kommer in och och frågar hur länge vi ska hålla på)

MJ: liten liten stund.

M: Hur allmänt ser du på att kunder inte vet om säkerhetsproblem? Hur ser du på små och stora företag?

MJ: det är nog just fråga om specialisering. Jag träffar ju inte kunderna jättemycket men däremot försöker vi ju förstå dem, vad de gör och vilka krav vi ser på oss. Det är snarare att vi får specifika krav på en produkt, kan det vara för en kund, men oftast har de läst en standard från deras kunder. Såatte, större kunder har större möjligheter och bättre koll, ja. de har oftas personer som är specifikt utsatta för säkerheten. Sen finns det nischade företag som är extremt kunniga på det här och är experter som har startat ett företag. Men ju större, givetvis har de större möjligheter.

M: så det är beroende på bransch?

MJ: det ska jag nog också säga, eh det finns många kunder som bara använder det, de vill bara att det är krypterat så ingen kan avlyssna och bryr sig inte särskilt mycket om nycklar. Det ska bara funka. Men som sagt jag jobbar ju mer med infrastrukturen internt än externa kunder.

V: skulle du säga att säkerheten har en större betydelse nu än för några år sen?

MJ: oja definitivt! Mycket fler hot i och med våra moduler går ju ut i miljontals exemplar och samtidigt så har vi ju andra tillverkar. Tar du de här enheterna så kan du ställa till med väldigt stor skada på internet eftersom de kan skicka stor mängd trafik. Vet du exakt vad du ska göra, finns flera fall där detta har inträffat, bland annat har man använt IoT devices för att sänka nätverksinfrastruktur på global skala.

V: finns det några nämnvärda fall?

MJ: det gör det. Men kan de inte direkt ur huvudet men man kan googla.

M: men vad gör ni för att säkerhetsställa att detta inte skulle hända för era produkter?

MJ: där har vi Secure boot, ett av våra koncept där vi ser till att det bara är u-Blox mjukvara som kan köras och om nån modifierar den då ska säkerheten säga nej detta är inte längre u-Blox mjukvaran och då stänger vi av helt enkelt.

M: men finns det kunder som säger att de inte vill ha på detta sättet?

MJ: finns ju de som gör sin egna lösning helt klart, eh, och det har vi ju moduler för. Såatte då får de en helt tom modul och får inte med våran säkerhet och då kan de lösa det själva.

V: har ni någon strategi att se till att de är medvetna om vilka risker det finns?

MJ: inte vad jag vet på så sätt men jag vet att det är en löpande diskussion med varje kund.deOftast är säkerhet lite speciell på så sätt att beställaren har ibland med sig en expert som kan de här bitarna eller så har de med sig en branschstandard och säger att detta ska uppfyllas. Men just säkerhet i sig är en specifik specialkompetens. Vilket gör att ska man förstå hur allt hänger ihop så måste man i princip uteslutande jobba med det. Man kan jämföra med vår certifiering av radio. För att du ska få lov att använda den måste du vara certifierad och många beställare vet inte om vilka krav som finns på radiostandader men de vet om att de behöver det. Och jag tror det blir samma sak för säkerhet.

V: den här frågan kanske är lite för teknisk för oss men hur är era produkter i kapp med hackers, det blir bara mer avancerat varje dag? Det är uppenbarligen något ni tänker på. Hur går det till och tänker ni då?

MJ: vi jobbar ju tillsammans med andra säkerhetsföretag då som är uteslutande experter på detta då. Så exakt hur vi gör håller jag lite hemligt.

(gemensamt skratt)

V: ja såklart.

MJ: men det är ju så att vår specialistkunskap är på radio och våra produkter, säkerhet är en del av detta och då finns det företag som uteslutande jobbar med att hålla koll på marknaden och senaste attackerna och liknande, så vi har samarbete med såna företag. Det för att säkerhetsställa att vi får den bästa rådgivningen och att vi kan med det i våra produkter. Det är ett jättejobb.

M: och kostsamt är det kanske?

MJ: det är det verkligen.

M: det diskuterade vi innan med din kollega Mats hur kunder ser på att betala några kronor extra per produkt för att få säkerheten men det kanske inte kunder tycker är värt.

MJ: det är oftast då det kommer ner till certifieringar och att det ska följa branschstandarder. Och det finns olika certifieringar du ska ha för dina produkter men det innebär också ett problem att du bara är certifierad ett kort tag för att sen kanske det kommer ut en ny läcka och då måste certifiera om. Det är ett ganska standard problem.

V: skulle det finnas en nackdel om u-Blox använde sig av uppkopplade produkter på företaget, skulle ni se det som en jättestor risk eller?

MJ: ja definitivt. Vi gör säkerhetsanalyser på vad som är skyddsvärt så det finns en metodik då man gör detta som heter threat modelling och då tittar man på hur, vilka attack ytor som finns, försöker minimera dem. Om vi ändå måste vara tillgängliga måste vi se till att säkerhetsställa de som loggar in. men vi får göra en modellering av de hoten som finns. Och se till att de är i olika sektorer.

V: vi har fått reda på att ni inte använder er av uppkopplade produkter utan tillverkar dem och ser till att ni skapar i princip säkerheten åt företagen, det är det vi undrar över.

M: ja och att ni har ett ansvar i detta. Ni ser fördelen med säkerheten och kunder kanske inte gör det, hur ser du på det ansvaret?

MJ: det blir rätt så enkelt för oss därför vi tillhandahåller en produkt och vi förklarar. Sen utöver det så är det svårt att ge några garantier men säkerhet är något fortlöpande. Så vi måste bygga in i vår arkitektur att vi kan ha uppdateingar, att vi kan spåra vart det är som går fel, att vi har en övervakning av marknaden. ehm , sen att vi följer de best practises, hur hanterar man nycklar, när byts de ut och så. Så om vi tillhandahåller den garantin, att vi gör det bästa vi kan på detta eller att vi uppfyller nån certifiering kanske kommer lite senare, då är det det vi garanterar.

Men i dag har man insett att säkerhet går att garantera så att den är en form av kostnad. Så vad kostar det att attackera en produkt? För att knäcka en produkt, det går idag, det är inte omöjligt men frågan är vad det kostnaden är och vad är då billigast och vilken motivation har denna personen. Så om man delar upp det, man kan ha enskilda hackare som kan sitta och vara väldigt duktiga eller nybörjare som använder standard verktyg de ska inte kunna hacka. Sen kan du ha företag som kontraspionage och då vill man gå in och säkerhetsställa att man inte blir utsatt för detta och att vi ser till att blockera sådana attacker som kommer. Sen har du då statligt intång, då börjar kostnaderna bli för höga, blir svårt att komma åt information. Finns många sätt att attackera. Då får man helt enkelt definera kostnad.

V: hur ser du på framtiden gällande utvecklingen av IoT produkter? Hur tänker ni? Vad är nästa steg?

MJ: som jag ser det måste vi ha säkerhet, vi kan inte inte ha det. Sen måste vi göra det lättare för kunderna att skydda sig och i takt med att chippen blir mer och mer avancerade och har mer säkerhetsfunktioner så får vi börja använda dem helt enkelt och se till att vi har metoder för att uppdatera våra kunder och när en läcka händer och inte om det händer. Hur hanterar vi det så att inte kostnaden bli för stor.

Tex xbox kan man knäcka nycklarna och spela piratkopierade spel men nu har xbox vissa säkerhetsfunktioner som uppdaterar mjukvaran så modifierar de chipen på så man kan inte backa bak och då har man täppt till några luckor. Det handlar om att försvåra hela tiden. Täppa igen luckorna. För de finns där. Det handlar om att hitta dem.

Man vill gärna ta tillbaka allt så det handlar om en kryptografisk säkerhet därför att det är väldigt svårt att bryta, ingen som kommit på hur man gör det än om man använde säkra nycklar och säkra nyckellängder. Men hårdvaran går att knäcka. Så kan du rensa bort plasten och metallagret

på chipet och sen kan du men avancerade mätinstrument då gå in och läsa ut innehållet istället eller bara läsa trafiken. Finns många olika sätt att få ut nycklarna ändå. me n då börjar vi prata kostnader, en 100 000 dollar, 1 miljon dollar. Är det då värt det?

M: från er produkt till molnet, var ser du är den största säkerhetsrisken?

MJ: oj ja. Det beror på vad du är ute att attackera helt enkelt. Vi pratar om assets, vad är det som är skyddsvärt eller är det slutet, själva noden. Om du tar bot nätverk för att använda d-dos attack när du ska slå ut internet då är själva end-noden det intressanta. Och det kan vara svårt att komma åt de via luften så då köper man en modul och försöker knäcka nyckeln som vi pratade om tidigare. Och det kan vara värt det. Om vi säljer 100000 moduler och de knäcker vår nycker och laddar upp en ny fejkad mjukvara och hittar ett säkerhetshål då kan de bara söka efter dessa enheter över nätet och när de hittar de så utnyttjar de svagheten och kidnappar dem. Det kostar rätt så lite. Men tar du skyddsvärd information som patientinformation i exempel ambulanser får information, eh, SSL certifikat, säker uppkoppling, det är säkert, det är inte så mycket man kan komma åt då. Då anske man kan gå på den ena modulen, i den första uppkopplingen till expempel, att där finns nån öppen dörr. Sen är det npg databaserna och runt molnet. Försöka hitta ett hål i mjukvaran där den behandlas, men även de är säkra idag. De har ett större perspektiv på säkerhet. Det är svårt och säga var man ska slå sig in. man får nog ta ett specifikt case isf.

V: vad är största risken för er med IoT produkter? Vad är mest utmanande?

MJ: ja ja. Nämen det är säkerheten, styrkan, hur ska jag uttrycka mig, den svagaste länken - var sitter den nån stans. Vi har många produkter som går ut till kunder, det är inte alltid kunderna kan uppdatera, så hur hanterar vi de produkterna. Ehm. det är nog helheten. Hela tiden försvara oss mot de hot vi inte känner till.

V: svårt att veta.

MJ: ja detta är ju första produkten som Malmö lanserar med säkerhet inbyggt dvs det finns säkerligen saker vi inte har tänkt på. Och hur hanterar vi dem. Beror ju på var de ligger nånstans. Nu är produkerna säkra i sig men om man upptäcker något som gör att vi behöver uppadatera nått, worst case scenario är ju om en nyckel läcker. Då måste alla kunder eventuellt byta ut sina chipp. Och det är det värsta som kan hända. Kanske inte den största risken men.

Funderar på kostnaden, det är också det som definierar säkerheten. Säkerhet är som kvalite, vad är kunden beredda på att betala. Och det är inte förrän det inträffar som kunden är beredd att betala och då är det redan försent.

V: det har varit återkommande för oss att det måste ligga en ekonomisk grund.

M: också intressant om kostnaden av minne och kapacitet, är det värt att lägga minne på en ex en tvättmaskin.

MJ: oftast kanske det inte är informationen i sig utan att man kan utnyttja som här enheterna i massiva attacker. En sån här liten enhet *(visar en av deras små moduler)* kan skicka ut tusentals paket och hittar jag ett hål i en av dem i en viss mjukvaruversion då kanske det finnas 10 miljoner enheter ute för dem kopplar upp sig mot nätet och det kan jag hitta vilka versioner de här är. Så då börjar man leta efter dem och sen kopplar du upp mot dem, modifierar dem och sen är de en del i din zombie armé. Vi pratar om att det kommer finnas miljarder av sånna enheter. Du kan sänka länder. Idag behöver du bara ha en enkel telefon för att slå ut ett helt windows nätverk. Så om nån kommer in här kan man slå ut nätverket för samtiliga enkelt bara med en telfon med vanlig 3G uppkoppling, behöver inte vara särskillt myckt traffik. Men vet man exakt hur man ska göra så kan man vara väldigt elak.

E: jätteobehagligt.

MJ: ja. Det finns några fall som kan vara intressanta. Ni har Philips Hue. sök bara på d-dos och IoT devices så hittar ni dem snabbt här fallen som finns.

M: d-dos?

MJ: distributed denial of service. Det är när du har massvis med enheter. Titta på vad kostnaden är. Om ni tar en sån här enhet och skalar chippet och skickar det till en firma som kan läsa ut det beroende på var det är för nått. Kanske köper 30-100 sådana moduler och får ut lite information. Eller så kopplar man upp dem mot ett kraftfullt kyloskåp (?) och så mäter man strömmen när den läser och då kan man se subtraktion, division, multiplikation, division som tar olika mycket ström och vet du då när den läser nyckeln så kan du i princip läsa av nyckeln. Så det finns lite olika sånna här attacker. Du kan gå på chipp tillverkaren, byta ut chippen och så. Ta ett par sånna scenarion och titta på vad är kostnaden om du ska köpa 100 miljorner datorer som ska delata i et d-dos attack för att sänka ett företag och utpressa dem. Ta amazon, hur mycket tjärnar amazon på en dag? Kan vi sänka dem med det här? Eller ta kanske u-Blox strolek, då pratar vi miljorner varje dag. Om du du köper 100 miljorner sånna här enheter ja då knäcker du nycklarna och sen så använder du dem. Det är den ekonomin som finns.

M: det är det som kan vara den bakomliggande tanken.

MJ: ja percis. Ingen skulle bry sig om säkerheten om det inte finns nån ekonomi i det.

Alla instämmer

MJ: vore intressant att se en formel från er sen.

Alla skrattar lite och instämmer.
V: det är intressant och se hur företag prioriterar säkerhet.

M: för om det är något som företag är mån om är det pengar. En onödig kostnad om det går snett.

MJ: tillförlitlighet är ju också en sån sak. Säkerhet har med tillit att göra. Har man då en gång hanterar det dåligt ät det svårt att få tillbaka tilliten.

M: och då förlorar man också pengar om ens kunder inte litar på en.

V: verkligen. Det är nog detta vi har annars. Vi har redan pratat med Mats om hur ni u-Blox tänker om säkerhet etc.

MJ: Mats är bra på att svara på det.

M: det var intressant det här lite mer tekniska som du har berättat. För det har vi inte riktigt gått in på.

MJ: har ni fråga gällande det mer tekniska så hör av er. Finns många attacker och nycklar man kan prata om länge. Kostnader finns idag för att vara säker, attackerna blir bättre och bättre.

M: men det handlar först och främst om kryptering för er?

MJ: ja i grund och botten går det alltid tillbaka till kryptering. Säkerhet har tre saker, en triad, det ska vara confidentiality, integrity och availability. Och det är hela tiden en balansgång.

M: går ni mycket efter CIA?

MJ: ja vi specificerar för alla våra assets vilka krav som finns från ett säkerhetsperspektiv. Sen finns det en rad andra attribut som man kan lägga ovan på, som att access ska vara autentiserad och att personen ska ha rättigheter. Alla dessa saker måste du definiera. Det blir en formell process.

MJ: ni får maila om ni vill veta mer.

V: vi lär maila.

MJ: när ni kommit längre så kan vi gå ner i fördjupning och detalj.

V: men tack så mycket!

MJ: lycka till!

Bilaga 5: Intervju LTH

Transkribering 4

Intervju med Martin Hell, docent i informationsteori och lektor i datasäkerhet	
Datum:	23-04-2018
Tid	09.06-09.45
Intervjuare	Emma Nilsson (E), Matilda Stading (M), Victoria Andersson (V)
Intervjuperson	Martin Hell (MH)

Transkribering av den andra intervjun på LTH, Måndag 23 april. I E-Huset tillhörande LTH i Lund på intervjupersonens kontor.

E: Emma Nilsson
M: Matilda Stading
V: Victoria Andersson
MH: Intervjuperson, Martin Hell, docent i informationsteori och lektor i datasäkerhet

V: Vi hittade dig genom en artikel från förra året och ditt projekt och vi blev jättenyfikna!

M: Aa, superbra!

V: Ehm.. men ja, annars är vi två skåningar och en göteborgare

(gemensamt skratt)

M: Vi försöker samla in all empiri vi kan få!

MH: Ja, var är ni nu i ert arbete? Är ni halvvägs eller?

E: Mer än halvvägs skulle jag säga.

M: Ja, vi har inlämning inför förseminarium nu denna veckan.

MH: Okej.

M: Så det är i sluttampen nu så vi ska gå igenom det och så.

MH: Har ni skrivit ner vad ni har kommit fram till i på de andra ställena ni har varit på?

M: Aa, lite halvt har vi väl kommit fram till…

V: Vi har ju suittit och transkiberat..

M: Ja, usch ja…

(gemensamt skratt)

V: Så det är… man blir ju trött på sin röst ehhh, och den andres.

M: Men, jag tycker att det låter ganska lika faktiskt emm…

E: Ja, och det är intressant hur säkerheten har kommit så sent.

MH: Vad säger de om det? Det skulle vara intressant för mig att veta också.

V: Ja, det är väl någon slags kommunikation att det är någon slags trend och att attacker har hänt och man har tänkt i efterhand, det har absolut inte varit någon prioritet ehh, innan utan man har prioriterat funktioner istället för själva säkerheten.

MH: Mm, precis. Man det är fortfarande inte svar på frågan varför det kommer nu..

V: Nej, precis och det är väl såhär, och det är det vi vill veta också.

E: Men, det är intressant också, vi snackade med något företag som nämnde utbildningen, att redan där är säkerheten i andrahand så vi lär oss på något sätt att utveckla och designa först innan vi tänker på säkerheten. Och, många utbildningar inte ens säkerheten med så hade vi haft säkerheten redan från första början så hade det kanske inte sett ut som det gör idag, eftersom det kommer i efterhand redan där liksom..

MH: Ja.

M: Så det är super intressant och höra vad du säger om detta också!

V: Ja, du har frågorna där va? Men, vi skulle först framförallt veta vad det är du gör. Vi vill veta om projektet lite briefly, men din titel, vad du gör här som vad heter det…

MH: Min titel, min tjänst är ju lektor men min titel är docent så de skiljer på det i den akademiska världen.

V: Ja.

MH: Eh, men jag är docent i informationsteori och lektor i datasäkerhet, det är skillnad när det kommer till…

M: Okej, okej, aha.

MH: Jag diskuterade för, 11 år sedan i kryptering så jag sysslade med mycket matematiska aspekter i krypteringsalgoritmer. Både tillverka och kränka dem som redan finns.

V: Ja.

MH: Så det är väl min bakgrund. Sen efter det gick det över mer till säkerhet fortfarande lite kryptering håller jag på med men det har glidit över mer och mer på säkerheten för de flesta av mina doktorander sysslar med säkerhet, uteslutande med ren säkerhet. Där är någon som sysslar lite med kryptering fortfarande men det är, ehh. Och säkerhet, mjukvarusäkerhet har jag gjort en del, emm. Trusting computing, har jag gjort en del. Men mycket åt mjukvaruhållet och så lite olika aspekter på det, både tekniska och kanske lite mer otekniska på den senaste tiden.

V: Ja, intressant. Eh, jag vet inte om vi har någon ordning på frågorna.

M: Jag hittar förlåt inte frågorna…

V: de ligger bland research bland intervjuer. Men…

MH: Vi ska inte ha sånt mellansnack, det måste ni ju transkribera det med.

M: Ja, precis.

V: Ja, vi får skriva paus.

(gemensamt skratt)

V: Okej, men då skulle vi vilja veta lite mer om det här projektet seconds.

MH: Ja!

V: Eh, som du startade i samband med olika företag och studenter.

MH: Ja. Nej, det är lite studenter också det är det ju men det är framförallt företagsnära projekt. Det är ju finansierat ut av Nova som är en av sveriges största finansiärer. Och, de finansierar ofta projekt som är väldigt nära företag, nära näringslivet, asså man ska hitta lösningar som företag faktiskt har riktigt nytta av. Om man jämför med kundforskning så liksom, en grundläggande frågeställning som man kanske har nytta av 10, 15, 20 år fram i tiden så är detta någonting som faktiskt är nära hur företag arbetar nu. Då såg vi det här som ett problem, just det här med säkerheten i IoT, det kommer många fler IoT enheter och hela tiden, flera miljarder om året som man lägger till i antalet enheter. Samtidigt börjar man använda massa tredjepartskod som där

funktionaliteten har identifierats, den kommer i första hand och den kommer antagligen att komma i första hand i lång tid framöver. Och för att slippa utveckla all kod själv så plockar du in kod som någon annan har gjort så du tar open source kod och lägger in i dina produkter sen lägger du till lite egen funktionalitet och då har du en produkt. Och så kan du skeppa ut den väldigt snabbt och då finns det många produkter på marknaden som har öppen källkod och sårbarheter. Och den måste uppdateras. Och det är det problemställningen är.

V: Är det det som är nackdelen med open source, att det finns massa svagheter i att man inte har någon koll på koden, eller vad..

MH: Nej, det kommer definitivt att finnas den här typen av sårbarheter i din egna kod som du utvecklar också.

V: Okej.

MH: Skillnaden är att, din egna kod kommer inte att ligga känd för alla i någon databas men det kommer den här öppna källkoden att göra. Och den egna utvecklade koden kommer inte att vara gemensam mellan jättemånga, flera miljarder enheter runt om i världen men om alla använder samma öppen källkod för sina produkter så kommer du ha samma kod i flera miljarder olika enheter. Får du då ett säkerhetshål i den så kommer jättemånga fler enheter att påverkas än om ett enda företag, i sin egen kod har en sårbarhet. Så dels är det mer som påverkas och lättare att hitta och lättare utnyttja också för när de ska skriva en exploit till en sårbarhet i ett av de här biblioteken som är öppna då så kan ju vem som helst använda den här exploiten då ju. Om de gör den fritt tillgänglig. Men det kanske inte finns samma incitament att skriva en exploit och göra den fritt tillgänglig till en mindre mängd enheter och mindre mängd är kanske fortfarande 100 000, eller något sånt där. Det är ju mycker mer begränsat.

V: Skulle du säga att det är vanligt att företag använder sig av öppen källkod för att göra det lättare för dem själva? Eller?

MH: Vad sa du? Att analysera eller använda?

V: Att använda.

MH: Jaja, det är jättevanligt.

V: Det är det?

MH: Jaja, det finns nästan inget företag som inte använder open source kod någon gång, eller någonstnas. Det finns enstaka exempelvis, vissa jättestora företag som har hög industriell säkerhet och industriell produktion, möjligtvis att de inte, att de vill ha egenutvecklad kod. Men ser du de mindre företagen som poppar upp nu de kan ju inte implementera sina egna operativsystem eller sina egna nätverksstackar eller sina egna webserver utan de tar ut av det som är fritt tillgängligt.

M: Varför tror du att det är så då?

MH: Det är kostnader framförallt. Du kan inte göra det själv, det finns ju inte så många utvecklare heller så varje sånt här litet företag skulle ha en egen utvecklare för att göra allt detta. Det finns ju redan brist. Jag tror att jag så någon siffra på 750 000 utvecklare som saknades i EU för tillfälligt, och det är ju ganska många.

M: Ja, verkligen.

V: Nej, det är helt otroligt vilken branch. Men, vad skulle jag säga. Skulle du säga att kostnaderna är anledningen till varför säkerheten inte är där den skulle varit idag? Jag tänkte, för andra företag som vi har pratat med de säger att tekniken finns, men inte pengarna.

MH: Tekniken för?

V: Nej men asså, för att se till att man kan skydda olika enheter.

MH: Jaja, den finns, den har funnits jättelänge. På sätt och vis i alla fall. Det finns teknik för att göra det säkert men samtidigt när du utvecklar ny teknik så utvecklar du ny kod och då kommer det finnas hål i den koden också.

M: Mm..

MH: Men det är ju klart. Många av de attackerna vi ser idag, många av de sårbarheterna som vi ser idag vet man ju sedan länge tillbaka. Att det här är bara dumheter som man sysslar med. Asså, det är ju jättelätt att skydda sig mot detta.

M: Men är man inte rädd för att det ska bli ännu, asså de som gör attackerna, att det ska bli ännu smartare, eller vad man säger, smartare datorer med större kraft och sånt. Att säkerheten på något sätt inte ska hänga med.

MH: Asså säkerheten i produkterna, den hänger nog inte med mycket på grund av, jag tror att det är mycket på grund av kunskapen hos företagen. Asså om du ser de här enkla attackerna som du ser i tidningarna, de jättestora attackerna. Det är oftast väldigt enkla saker som man har känt till under många år hur man ska lösa de här problemen. Bara det faktum att man skickar kommunikationen okrypterad det har vi ju känt till sen 60, 70 år tillbaka att det ska man inte göra och ändå så skickar man det okrypterat idag och där så har vi en stor kundskapsbrist. Men sen, om du tittar på andra säkerhetshål när det gäller uppdatering det är ju mycket kostnader. Snabbt in med koden, snabbt ut med ny funktionalitet, vi måste konkurrera med andra och vi måste därför ha bättre funktionalitet än de andra. Kunderna bryr sig inte om säkerheten så mycket, de vill ju ha en viss funktion. Om ni ska jämföra två mobiltelefoner, samsung och iPhone, det är de enda jämförelsen ungdomar gör idag. Vad är det ni jämför? Jämför ni säkerheten eller är det något annat ni jämför? Det är ju ni som är kunderna, det är ju ni som bestämmer, det är ni som genererar intäkter. Om det är ett jättestort säkerhetshål i en iPhone, och den inte finns i Samsung, skulle ni sluta köpa iPhone då? Nej, det skulle ni inte.

M: Nej…

MH: Så konsumenterna bryr sig inte. Man snackar jättemycket om integritet, eh, facebook när man delar med sig av information och gjort det till en jättestor grej. Och så går man ut och frågar människor, de är ju jätteglada för att dela med sig av information. Ni använder facebook, ni använder instagram, ni använder bloggar, ni gör video och youtube filmer och delar med er av all information. Inte er personligen då såklart men ni delar med er av så mycket information ni bara kan. Tar selfies tre gånger i timmen och lägger upp det och säger exakt vad ni åt till middag och fotograferar den middagen. Jättenöjda med att lägga ut allt om era liv och sen så kommer man och tycker att detta är ett jättestort problem i samhället samtidigt. Det sker någon form av konflikt där som vi fortfarande måste ta och reda ut.

V: Skulle man rent konkret kunna säga att luckan som uppstår och den här kunskapsbristen som finns på företag och att man vill hänga med i den vågen att man ska ha bäst funktionalitet, man ska hinna med varje trend? Skulle man kunna säga att det är en lucka mellan de eller är det flera faktorer i det?

MH: Nej, nej! Det är ju en stark konflikt mellan det.

V: Ja…

MH: Asså, det som styr idag är ju funktionaliteten vi måste ha ut snabbt på marknaden kommer du inte ut snabbt på marknaden med din produkt så kommer konkurrenterna att göra det istället och företagen kommer att försvinna. Så fort man börjar hamna efter, ni ser ju Nokia, Nokia var världsledande när det gäller mobiltelefoner men de hängde inte med när det gällde smartphones. Och.. vips så var de ett marginaliserat företag. Och, där var bara funktionalitet som styrde. Men, vad var skillnaden i säkerhet mellan Nokia och de andra telefonerna? Det var ingen som brydde sig…

V: Nej…Vad tror du att konsekvenserna kan vara?

MH: Konsekvenserna där var ju inte så stora med tanke på att tiden såg annorlunda ut då men konsekvenserna nu kommer vara annorlunda. Nu har du ju liksom IoT enheter, små sensorer som ska placeras ut precis överallt och övervaka allting i samhället.

M: Mm..

MH: Och även om fortfarande funktionaliteten är drivande idag så kommer säkerheten att få en helt annan impact än vad den hade tidigare. För nu är det inte en person du attackerar när du hittar någon sårbarhet i mobiltelefoner, om vi fortsätter med det exemplet, så är det inte längre en person du attackerar. Men hittar du sårbarhet i kanske en produkt som ska styra kritisk infrastruktur eller hittar sårbarhet i något som styr hur trafikljusen fungerar. Då är det inte längre en person som kommer att drabbas av att dagens maträtter läckte ut till fel personer utan nu är det någon som sitter och styr trafikljusen och sätter alla på grönt för att de känner för det och kommer därmed att skapa stor kaos i samhället och jättemånga blir drabbade och påverkade istället. Så, konsekvenserna idag är ju helt annorlunda än vad konsekvenserna var förr i tiden.

V: Hur tror du att man skulle kunna få företag att bli mer medvetna? Från dig personligen.

MH: Företagen är medvetna om det..

E: Ja, de bara struntar i det?

MH: Jag tror inte att de struntar i det egentligen, de vill göra detta med det saknas, dels så saknas det incitament att göra det än så länge men incitamenten är på väg att komma. Och det är ju det ni har sett också det har ju verkligen hänt någonting de senaste åren. Det finns ett helt annat incitament att göra det för nu när ditt företag blir utsatt för en attack så är det liksom inte de här små sakerna som händer utan nu kan det faktiskt vara väldigt stora konsekvenser av det. Men det är ju som i tidninge, att Ryssland håller på med cyberattacker mot era routrar, det gjorde de kanske inte för tio år sedan.

M: Det har vi sett som en trend, att det är mer viktigt med säkerheten för att de själv kommer att förlora mycket pengar om deras produkt kommer bli attackerad eller någonting. Vi fick höra till exempel om IKEA faktiskt, att de har gjort såna smarta lampor och hade gett dem till en konferens så att de fick hacka det. Typ sånna grejer kommer ju att hända men det är ju inte tillräckligt men jag tänker på företagen som du har i ditt projekt, hur ser du en trend mellan dem typ?

MH: Nej, det är lite olika mellan olika företag. Om man tar eh, jag kan inte säga för mycket hur de arbetar internt men asså det vi kan se att på senaste åren så har ju säkerheten prioriterats på ett helt annat sätt. Asså, vi började det hä projektet någon gång 2015, tror jag. Och på den tiden, på några företag, så har det hänt jättemycket gällande säkerheten så det har varit en helt annan prioritet nu. Om det är på grund av projektet eller om det är på grund av yttre omständigheter, andra omständigheter det kanske är svårt att säga men man märker att det är jättemycket större med säkerheten. Tittar du nu på vad företag vill anställa idag så är ju säkerhetsexperter liksom det som är kanske är det en av de sakerna där du får lättast jobb. Det finns andra där du får ännu lättare jobb men..

E: Utvecklare kanske?

MH: Ja, eller kan du machine learning så har du jobb inom fem minuter.

M: Vad är det för företag som är med i projektet?

MH: Eh, de stora är Axis, Ericsson, Prevas ganska stora, vi har ett företag i stockholm som heter T2-data, vi har Sensative, sen har vi Advenica som är ett säkerhetsföretag i Malmö. Så det är se stycken företag och så är det vi här på LTH sen så är det Sics Rise, Rise Sics som är ett forskningsinstitut som är, som finns i Stockholm och ja, de har en hel del säkerhet här i Lund också.

V: Och, det är företag som ni hjälper? Eller jag kommer inte ihåg…

MH: Asså, projektet handlar liksom mer om att vi sitter kanske och gör saker här och sen får vi feedback av företagen. Företagen gör saker på sitt håll och sitter och implementerar sina saker och sen så försöker vi koppla ihop de sakerna som vi, och de sakerna som de gör. Så att vi får liksom en hel kedja när det gäller att hålla koll på sårbarheter. Från liksom första att du börjar identifiera ny sårbarhet tills att du faktiskt har patchat en i slutändan och mellan det så går det ju flera steg. Vi försöker få ihopa de stegen på ett bra sätt så att man får ett bra arbetssätt för att göra detta så att man inte missar saker på vägen. Dels att effektivisera olika delar i processen och dels se till att de inte missar några viktiga saker på vägen framåt.

M: Så det är nästan på väg till en standard typ eller en praxis?

MH: Njaa.. asså praxisen. Man kan ju egentligen säga att mycket av praxisen finns redan det är bara det att den ska användas också. Så det vi försöker göra är att möjliggöra för företagen att bättre använda de praxisen, skulle man kunna säga. Så asså, att sårbarheterna finns, vi hjälper inte till att hitta sårbarheter i deras egen kod till exempel utan vi hjälper till att effektivisera deras arbete för att hitta sårbarheter i den kod som de plockar in från tredjeparter. Och analyserar de sårbarheterna hur de faktiskt skulle påverka deras produkter. Så det är där vi försöker förbättra deras processer med hjälp av olika verktyg.

V: Skulle det finnas någon möjlighet att ta del av den standarden? Att få reda på mer om processe, hur den ser ut från början till slut?

MH: Ja, asså ni kan ju titta, ni kan ju titta, på såna härа modeller som finns redan, vi håller på att göra en egen modell men den är inte färdig ännu, som är lite mer fokuserad på sårbarhetshantering. Men där finns en del modeller som ni kan titta på, b simm som är jättevanlig. B S I M M.

V: Okej, då gör vi det.

MH: Sen finns det en som heter samm, SAMM, tror jag att den heter.

M: SAMM.

MH: Ja. Och det handlar mycket om liksom att arbeta med säkerhet över huvud taget på företag. Hur företag ska göra för att arbeta med säkerhet, i olika kontexter. Och sen så, det vi försöker göra är att ta delar av de här, eller ett delprojekt som vi gör kan man säga. Där försöker vi ta delar av det här och sen så lyfter vi ut delar som har med sårbarhetshantering att göra och så försöker vi expandera detta så att det blir mer rigoröst än vad det är i de här modellerna. Få med fler delar och göra det tydligare för företagen. Så det är ett delprojket som vi sysslar med.

M: Och är de här modellerna någonting som är asså väldigt viktigt i säkerhetsarbetet?

MH: Jag tror att det är många företag som utgår från de här modellerna. Det är ju ganska bra, man behöver kanske inte följa de slaviskt men man kan ju titta vad det står i dem. Se så att man inte missar något. Var ska vi vara i vår organisation i olika aspekter för att hålla koll på säkerheten i våra produkter. Och på det sättet är de väldigt nyttiga.

M: Verkligen. Men vad tror du att.. Asså säg de företagen som kanske är tillverkande företag som gjort kanske brödrostar, om de helt plötsligt ska göra uppkopplade brödrostar. Var ser du liksom problemet, underliggande problemet, som ligger där?

MH: Asså säkerhetsmässigt?

M: Mm.

MH: Det underliggande problemet är ju typ det att de inte har den kompetensen i företaget. Så vill de plocka in den kompetensen, så finns det kompetensbrist generellt när det gäller den här typen av saker. Och då får du ju ett problem, du kan ju enkelt göra en uppkopplad produkt egentligen men då kanske du tappar säkerheten. Ja, så där har du ju, ungefär som vi var inne på innan det är ju ett mellanting. Det finns ju en kompetensbrist i samhället när det gäller de här sakerna och så finns det också… Ja, nu vill de göra en uppkopplad brödrost, ska jag få ut den uppkopplade brödrosten om ett halvår eller ska jag få ut den om fyra år? Då väljer de naturligtvis någonting tidigare. Och då ska det gå fort.

V: Ett av de företagen vi pratat med, de diskuterade ju att i och med att det är en stor kedja, det här med produkter och att, det företaget vi pratade med var ju U-Blox och de tillverkar ju moduler till företag och de försöker ju redan fokusera på säkerhet för sina små radiokommunikations små moduler.

MH: Det låter som U-Blox?

V: Ja! Exakt. Och undrar om du tror att det kommer vara väldigt vanligt sen när företag inte väljer att lägga pengar på kompetens utan väljer att fokusera på företag som bara fokuserar på säkerhet, eller främst på säkerhet.

MH: Det tror jag är en ganska bra väg framåt också. För att då får du någon for av, det får ju en fokusering på säkerhet bland de som kan säkerhet sen kan andra företag göra det de är bra på. Istället för att ta en person och sätta på det företaget, en person på det företaget, en person kan ju inte kunna allt ju. Så istället tar vi kanske 50 personer och sätter de på ett företag som hjälper de här olika 50 företagen och då kommer det ju bli väldigt mycket mer effektivt. Och det är ju så man gör i alla andra delar av samhället också asså man outsourcar de delarna som andra kan göra bättre och effektivare. Och det tror jag inte, det är ju inget unikt för det här, det är ju dit det kommer att gå såklart.

V: Ja.

MH: Sen är det ju.. Sen måste man ju ha en person som kan säkerhet på varje företag också för det finns ju någon form av daglig verksamhet där man måste hålla koll på säkerheten. Du kan inte bara outsourca allting. Du behöver faktiskt ha kunskapen i företagen också. För annars asså, du kommer inte ha koll på det, du kommer fallera.

V: Varför tror du, för du sa det innan vi började, liksom att, det är ju inget svar på varför det händer nu. Är det bara kunskapsbristen eller varför hände detta liksom inte innan? Jag tänker att tekniken har ju funnits länge och..

MH: Konsekvenserna har inte varit lika stora innan.

V: Vad sa du?

MH: Konsekvenserna har inte varit lika stora innan. Nu får det mycket större konsekvenser, du får ju hela tiden nya attacker som slår rekord på rekord hela tiden. Och attackerna blir större, du har ju jättemånga faktorer som samverkar. Dels så har du incitamenten bland de som attackerar. Förr i tiden så var det mycket mer av intresse, nu är det mer av ekonomiska skäl, du tjänar pengar på de här attackerna. Du har kompetensbrist, du har fokus på funktionalitet, du har mycket fler enheter ute. Du har mycket mer open source, du har många fler som arbetar med att göra ny open source vilket innebär att det det kommer finnas, asså det behöver mer funktionalitet när du ska utvecklar fler produkter, utveckla samhället på det här sättet. Och då måste du utveckla produkterna och då kommer det nya sårbarheter också. Så det är jättemånga saker som samverkar där hela tiden.

E: Intressant.

M: Hur tror du att framtiden kommer att se ut då? Med, inom IoT och säkeret?

MH: Ja, om jag visste det… Jag tror att vi fortfarande kommer att se mer och mer fokus på säkerhet, det känns så, jag tror kanske att vi bara är i början av den här fokuseringen som vi ser. Men jag tror ändå att vi kommer fortsätta att ha en stor kompetensbrist men vi kommer att se stora attacker framöver. Vi kommer se många attacker, vi kommer se allvarliga attacker. För 15 år sedan så körde man in flygplan i skyskrapor och nu kan man sitta framför en dator och släcka hela företag, eller nästan hela nationer kan man liksom få, mer eller mindre gå under. Så, det är stor skillnad på vad som krävs för att göra attacker. Det är enklare att gör attackerna och det blir mycket högre vinning på det också med mindre medel.

E: Ja, och dessutom så är du skyddad när du sitter vid datorn hemma.

MH: Potentiellt sätt så är du skyddad, ja.

M: Hur ser du på, asså myndigheters medverkan i detta? Till exempel så kommer ju GDPR nu och det handlar ju om integritetdelen men tror du att det kan vara en anledning till att säkerhet inte hänger med?

MH: Att… jag förstod inte frågan.

M: Jag tänker att eftersom myndigheter ändå har en makt och säger till företag att de ska följa den här praxisen eller standarden. Tror du att det kan vara ett problem asså att de kanske inte är tillräckligt medvetna?

MH: Att myndigheterna inte är tillräckligt medvetna?
M: Ja.

V: Att det kanske bromsar.

MH: Nja… jag är inte säker på att myndigheterna bromsar, de försöker nog driva på det här men det finns fortfarande inga riktiga straff för de som inte följer de regler som finns. Det kom ju det här nya EU direktivet som ser till så att du kan faktiskt bli, asså du måste rapportera sårbarheter om du är en viktig part. Så små företag behöver inte rapportera men stora företag måste då rapportera sårbarheter. Behöver en samordnande nationell myndighet som har hand om sårbarheter i olika delar av samhället. Så den saker kommer ju att driva saker framåt men du behöver ju ha riktiga incitament för företag för att göra detta. Och incitamenten finns du där men de är inte riktigt tillräckligt stora än, tror jag.

E: Men jag tänker typ på det, vi pratar mycket om det att det är kompetensbrist, asså kunskapen finns inte riktigt, asså den finns ju, men den finns ju inte så många. Vad ska vi göra åt det? Vad tycker du?

MH: Jag tror att man behöver utbilda på företag man behöver, asså företagen måste inse att olika människor i vår organisation behöver ha bättre koll på säkerheten. Vi kan inte bara säga till någon yttre organisation att ta hand om säkerheten åt oss. Man kan komma ganska långt på det men man kan inte komma hela vägen. Man måste se till att utvecklare runt om i organisationen har koll på säkerheten. De ska inte bara kunna utveckla, de ska ha koll på lite säkerhet också. Och där behövs det ju internutbildningar, och kompetensutveckling på företagen och man måste faktiskt lägga resurser på det. Och jag tror att man kan komma ganska långt med relativt små resurser där egentligen.

M: Typ som vadå?

MH: Ja, internutbildningar! Asså, du tar liksom olika delar av organisationen för att se till att i alla delar av organisationen så finns det någon som har grundläggande koll på säkerheten. Och som då.. På något sätt samordnar funktionen på sin del av organisationen. Så att det är utspritt över organistionen.

V: Vet du om det finns något företag som gör detta, asså som verkligen strävar efter att amen att vi fokuserar inte bara på funktionalitet utan även på säkerhet?

MH: Ja, asså i vårt projekt så är Axis ett jättebra exempel på det.

V: Axis?

MH: Ja. De har jättebra säkerhetsarbete och jobbar mycket med det här.

V: Ja, jag har försökt att få tag i dem..

MH: Ni får inte tag på dem?

V: Nej.. de är svåra.

M: Har du någon som vi kan fråga så hade det varit jättebra!

MH: De är rätt upptagna, så jag kämpar också med att få en…

V: Vi kan gå dit samtidigt!

(gemensamt skratt)

M: Det är någonting som många, eller de företagen som vi har pratat med innan, är att själva medvetenheten kan vara skillnad på både att det är ett stort företag och att det är ett specialiserat företag. Typ Axis. De jobbar ju med övervakningskameror och säkerhet är ju redan en del i deras tänk. Har du sett något sånt?

MH: Om storleken påverkar? Eller om nischen påverkar?

M: Aa!

MH: Ja, det är klart asså ett företag som säljer förtroende asså ett säkerhetsföretag säljer ju förtroende, Axis säljer ju i någon mening förtroende för de ska ju sälja säkerhetskameror som ska vara top of the line, som är det bästa du kan få. Det är ju Axis. Så det ligger ju lite i deras produkt att de säljer ju inte bara en hårdvara de säljer ju kvalitet också. Och kan då ta extra betalt på grund av att det är kvalitet de säljer. Då är vi tillbaka till iPhone, de tar ju mycket mer betalt än vad de orde men de säljer ju kvalitet. Och det är det folk förväntar sig och då måste man faktiskt mer resurser på den här typen av grejer, så det tror jag definitivt, att det finns den typen av aspekter. Många kinesiska företag kanske som framförallt säljer funktionalitet och inte säkerheten i kvaliteten.

M: Och de kan vara mer medvetna då?

MH: Ja, asså de är mer medvetna på grund av att det är en del av deras affärsstrategi. Inte på grund av att de är smartare eller sådär, det är en del av deras produkt att kunna sälja den här kvaliteten så då måste de ju plocka in den här kompetensen som måste ha fokus på de sakerna. Och då blir det ju automatiskt, då har du ju incitamentet. Du har inte incitamentet på många av de andra företagen att ha mer fokus på säkerheten. Men Axis har ju ett typiskt incitament att ha hög säkerhet.

V: Hur kommer det sig att du valde den här inriktningen, kryptologi och säkerhet, av alla inriktningar på elektro?

MH: Lång historia. Mest slump.

V: Intressant också?

MH: Ja intresse har jag. Tyckte signalbehandling var skittråkigt.

Gemensamt skratt

M: ser du någon trend bland dina studenter?

MH: Ja faktiskt ett högre säkerhetsintresse. Tittat man på våra fortsättningskurser så är det nog de kurserna som har flest studenter. Vårt paket med fortsättningskurser så har vi extremt många som väljer säkerhet. Jättestort intresse bland studenterna.

E: Jättebra att det börjar redan där innan man kommer ut på företag.

Personligt sidospår

V: Jag har en fråga om arkitekturen gällande IoT. Finns många olika saker som sägs om detta. Finns ju 3-skikt och 5 skikt. Hur skulle du förklara hur ett IoT system ser ut?

MH: De kan se ut på väldigt många sätt. Finns en RFC som beskriver olika typer av arkitekturer som ni kan titta på. Kommer inte ihåg vad den heter. Sök på RFC IoT architecture eller nått sånt. Finns lite olika arkitekturer...Hur enheterna kommunicerar med varann och kommunicerar via en gateway upp i molnet osv. Väldigt ad hoc ibland hur det är gjort men det är ganska vanligt att du har en enhet som pratar med en router, centralbox, och den routern i sig är kopplad till en molntjänst. Så pratar de med via den routern eller direkt utan routern i mellan. Olika med olika produkter beroende på man väljer att göra.

M: Tror du kan vara därför det kan finnas säkerhetsluckor på grund av det är olika arkitekturer?

MH: Det är nog inte helt omöjligt. Det finns inga tydliga standarder för hur du ska göra de här sakerna. Finns ganska mycker arbete med den här typen av standarder för att ta fram standardiserade protokoll för att kommunicera med en enhet. Det finns naturligtvis arbete kring det men man har kanske inte nått fram till en specifik standard, det är såhär vi ska göra och detta är det bästa sättet att göra det på. Och man kommer nog komma dit så småningom, så det svänger in sig åt det som är bättre. Det börjar med att det finns jättemycket sen så försvinner vissa saker så blir det bättre och bättre sen så har du några som kommer vinna det här i sluändan. Där kan det vara så att utvecklingen har gått lite för fort så man har inte hängt med att standardisera de här sakerna tillräckligt bra.

V: Tror du det kommer finnas såna standarder i framtiden? Att det kommer finnas en stor mängd att välja på?

MH: Både och. Det kommer alltid finnas mer än en, det tror jag och det behövs nog också. Det behövs konkurrens och tillräckliga skillnader mellan olika typer av scenarion för att du ska behöva olika standarder också. Men de här standarderna, som många andra standarder, finns för att säga till hur folk ska göra utan hjälper ju också folk att göra rätt. Så genom att titta på dessa standarder får du reda på att detta är det bästa sättet att göra det på. Bra men då gör vi det, så det betyder inte att man måste göra så men du får veta hur du bör göra. Så jättebra sak men den

typen av arbete. Att du har en mängd smarta personer som säger att gör så här. Då får man reda på att detta är det bästa sättet att göra det på.

M: Och detta är redan på gång?

MH: Ja finns redan en mäng olika standarder. Och olika situationer och olika företag som har detta och försöker promota det på olika sätt. Men kanske är nischade på olika sätt. Såna kan ni nog hitta på olika sätt. Några stycken i alla fall.

Alla: Tack!