



TEKNISKA HÖGSKOLAN
HÖGSKOLAN I JÖNKÖPING

**Massövervakningens påverkan på intresset
för öppen källkod**
Mass surveillance impact on interest for open source

Anton Nilsson

EXAMENSARBETE 2014

Teknikens tillämpning med inriktning
Datanätteknik

Postadress:

Box 1026

551 11 Jönköping

Besöksadress:

Gjuterigatan 5

Telefon:

036-10 10 00 (vx)

Detta examensarbete är utfört vid Tekniska Högskolan i Jönköping inom ämnesområdet Datanätteknik. Arbetet är ett led i kandidatpåbyggnadsprogrammet. Författaren svarar själv för framförda åsikter, slutsatser och resultat.

Examinator: Anders Adlemo

Handledare: Erik Gunnarsson

Omfattning: 15 hp (grundnivå)

Datum: 2014-05-23

Postadress:

Besöksadress:

Telefon:

Box 1026

Gjuterigatan 5

036-10 10 00 (vx)

551 11 Jönköping

Abstract

The year 2013 presented the largest disclosure of clandestine documents to date. These documents entailed information regarding global surveillance programs and their operation by intelligence-agencies such as the U.S NSA (National Security Agency) and locally in Sweden by NSAs counterpart the FRA (National Defense Radio Establishment). Furthermore, intelligence-disclosures revealed that large IT-companies participated in these surveillance-actions and actively shared user-data with the NSA. As a result of the disclosures there was an especially noticeable outcry from supporters of open source software who spoke out against these surveillance-programs as a gross violation of civil liberties. As a result of this a study felt appropriate to reveal if an interest towards open source has changed or become more representable within Swedish businesses.

The aim of this study is to evaluate if companies within the IT-sector consider global surveillance as affecting their business, as well to ascertain if open source is being used within the business-model, or if it has become a more representable option since global surveillance was disclosed.

An empirical study was conducted to answer these questions from a business and organizational standpoint by the use of interviews by randomly selected respondents. An evaluating questioners-guide was designed to promote candidness in the respondents' answers and opinions as well as to encourage discussions.

The result indicates that Swedish companies and businesses in general haven't implemented any major changes to their system architecture. They have instead opted to focus on revising their IT-security policies as well as adopting a new approach towards how management of sensitive files are to be stored and shared in a safe manner. The adoption of open source within businesses has grown in scale, and it is now considered a more acceptable alternative as well as a good basis to build applications and software upon. Companies with a very distinctive Microsoft-strategy however have shown some resistance in the adoption of open source, mainly because of high deployment costs, while maintain and asserting confidence towards their IT-suppliers. The essence of it all dictates that there may be a connection between global surveillance and an interest towards open source within the IT-sector, but that this is still somewhat premature to comment on as major changes in infrastructure take time to implement and that companies don't yet know how global surveillance will affect them in the future.

“The United States government has perfected a technological capability that enables us to monitor the messages that go through the air.... That capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything –telephone conversations, telegrams, it doesn't matter. There would be no place to hide.”

–Senator Frank Church, Chairman, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1975

Sammanfattning

Under 2013 skedde det hittills största läckaget av hemliga dokument. Dessa avslöjanden detaljerar den hemliga övervakning som genomförs av bl.a. amerikanska underrättelse-tjänsten NSA (National Security Agency). Offentliggörandet att stora IT-företag är delaktiga i denna övervakningen via samarbete med NSA har även framkommit. Förespråkare av särskilt öppen källkod ser massövervakningen som en inkräktan på den enskildes integritet. Därför är det intressant att ur en studiesynpunkt ta reda på om intresset för öppen källkod har ändrats eller är på väg att ändras på grund av de avslöjanden som skett i samband med avslöjandet av massövervakningen. Öppen källkod kan vara ett alternativ för företag som vill utforska lösningar utöver de traditionella och proprietära leverantörerna. Syftet med studien är att ta reda på om svenska företag anser att massövervakningen påverkar dem samt att undersöka om företag idag använder sig av öppen källkod eller om de nu överväger detta efter vad som offentliggjorts. Finns det en eventuell koppling mellan massövervakningen och intresset för öppen källkod.

Frågeställningar är som följer:

- Hur stor del av företagen i Sverige använder öppen källkod idag och hur stor del överväger att använda sig mer av öppen källkod?
- Finns det en koppling mellan avslöjanden kring massövervakning och intresset för öppen källkod bland svenska företag?

En empirisk kvalitativ studie har genomförts för att besvara dessa frågeställningar utifrån företags- och organisationers svar och åsikter från genomförda intervjuer med slumpmässigt utvalda respondenter. En intervjuguide med utvärderande frågor skrevs med ansatsen att ge respondenterna en öppenhet i deras svar.

Resultatet påvisar att svenska företag generellt inte tillämpat större förändringar inom sina system efter offentliggörandet av massövervakningen utan fokus har istället legat på att förändra sina IT-säkerhetspolicys samt ett förändrat synsätt på hantering av hur dokument sparas och skickas. Svenska företag använder generellt öppen källkod i större skala då det numera ses som ett mer accepterat alternativ samt en bra grund att bygga applikationer på. Företag som sedan tidigare innehar en utpräglad Microsoft-strategi är inte särskilt villiga att titta på alternativa lösningar utan förklarar att de har tillit till sina leverantörer samt att implementering resulterar i kostnadsfrågor. Sensmoralen är att det kan finnas ett samband mellan massövervakningen och intresset för öppen källkod inom IT-branschen men att detta ännu är något tidigt att uttala sig om då större märkbara förändringar tar tid att genomföra.

Nyckelord

- Massövervakning
- Öppen källkod
- Studie
- Intervju
- NSA
- FRA
- IT
- PRISM

Innehållsförteckning

1	Inledning.....	4
1.1	BAKGRUND OCH PROBLEMBESKRIVNING	4
1.2	SYFTE OCH FRÅGESTÄLLNINGAR	5
1.3	AVGRÄNSNINGAR	5
1.4	DISPOSITION	6
2	Teoretisk bakgrund	7
2.1	MASSÖVERVAKNINGEN.....	7
2.1.1	<i>Bakgrund</i>	7
2.1.2	<i>Tidslinje med betydande händelser</i>	7
2.1.3	<i>Politiska reaktioner</i>	8
2.1.4	<i>PRISM</i>	8
2.1.5	<i>Xkeyscore</i>	9
2.2	ÖPPEN KÄLLKOD.....	9
2.2.1	<i>Definition</i>	9
2.2.2	<i>Historik kring utvecklingsvägar</i>	10
2.2.3	<i>Fördelar och möjligheter med öppen källkod</i>	10
2.2.4	<i>Nackdelar och risker med öppen källkod</i>	11
3	Metod och genomförande.....	12
3.1	METODVAL OCH TILLVÄGAGÅNGSSÄTT	12
3.2	VAL AV LITTERATUR.....	12
3.3	DATAINSAMLING OCH ANALYS	13
4	Resultat och analys	14
4.1	RESPONDENTERNAS SVAR OCH ÅSIKTER	14
4.1.1	<i>Presentation av respektive respondent</i>	14
4.1.2	<i>Uppfattning om massövervakning och dess påverkan</i>	15
4.1.3	<i>Uppfattning om öppen källkod samt uppskattad användning</i>	16
4.1.4	<i>Säkerhetssyn på tjänsteleverans</i>	17
4.1.5	<i>Koppling mellan massövervakning och öppen källkod</i>	18
4.2	ANALYS	19
4.2.1	<i>Uppfattning om massövervakning och dess påverkan</i>	19
4.2.2	<i>Uppfattning om öppen källkod samt uppskattad användning</i>	19
4.2.3	<i>Säkerhetssyn på tjänsteleverans</i>	20
4.2.4	<i>Koppling mellan massövervakning och öppen källkod</i>	20
5	Diskussion och slutsatser	21
5.1	RESULTATDISKUSSION	21
5.2	METODDISKUSSION.....	22
5.3	SLUTSATSER OCH REKOMMENDATIONER	22
6	Referenser	23
7	Sökord.....	26
8	Bilagor.....	27
8.1	INTERVJUGUIDE	27

1 Inledning

Arbetet genomförs i samband med kandidatpåbyggnadsprogrammet på Tekniska Högskolan i Jönköping. Kandidatpåbyggnaden är ett påbyggnadsår som kan sökas efter att en av de tvååriga utbildningar som erbjuds genom JTH slutförts. Inriktningen på grundutbildningen för det här arbetet är datanätteknik. Datanätteknik är ett huvudämne vars fokus ligger på att administrera komplexa nätverk med hög prioritet kring säkerhet. Arbetet ska ha koppling till grundutbildningens huvudämne. I kombination med de senaste skandalerna som uppdragats kring massövervakning av Internet och avslöjanden om Sveriges inblandning genom FRA är ämnet av stort intresse och relevans.

1.1 Bakgrund och problembeskrivning

Under 2013 och framåt har flera större läckage skett från bland annat underrättelse-tjänsten NSA. Hemligstämplade dokument har släppts som avslöjar att USA bedriver en övervakningsverksamhet i stora delar av världen. Övervakning gäller kommunikation som sker i kabelnät och med luftburna radiovågor. NSA hävdar också att man har kapacitet och kunskap att dekryptera stora delar av den trafik som passerar hos NSA. Det har också kommit fram att flera större IT-företag har hjälpt NSA att samla in information och i december 2013 avslöjades även att svenska FRA är inblandat i massövervakningen. (1) (2) (3)

Avslöjanden om övervakningen har hittills huvudsakligen gällt enskilda politiker eller regeringar. (4) Efter dessa avslöjanden skulle det dock vara en rimlig misstanke att inte bara politiker och regeringar blir övervakade utan även företag. Detta på grund av offentliggöranden kring att stora IT-företag med tjänster som Hotmail samarbetar med NSA. (2) Svenska företag använder sig av Internet och mobiltelefonnät mer än någonsin samtidigt som externa IT-tjänster så som molntjänster och outsourcade lösningar ökar i popularitet. Flera av de populäraste molntjänstleverantörerna har på ett eller annat sätt dessutom visats vara delaktiga i massövervakningen och frågan är hur svenska företag då ställer sig i förhållande till detta.

Rörelser som ställer sig starkt frågande till massövervakningen är rörelser för öppen källkod som istället förespråkar öppenhet på Internet. Rörelsen är starkt kritisk till massövervakningen eftersom man anser att den inkräktar på den enskildes integritet. Inom rörelsen finns en uppsjö av olika projekt som strävar efter god säkerhet i sina mjukvaruprojekt och detta kanske skulle kunna vara ett alternativ som svenska företag kan tänka sig att utforska mer än de traditionella molntjänstleverantörerna på grund av avslöjanden som skett under 2013 och framåt.

För ett företag som erbjuder IT-tjänster kan det vara relevant att veta om intresset för öppen källkod har ändrats eller är på väg att ändras efter de avslöjanden som skett kring massövervakningsskandalen.

1.2 Syfte och frågeställningar

Syftet är att ta reda på om företag i Sverige tycker att massövervakningen påverkar dem, samt att undersöka om företag använder sig av öppen källkod idag eller om de nu överväger att göra det efter de avslöjanden som har skett. Finns det en eventuell koppling mellan avslöjanden om massövervakning och intresset för öppen källkod?

- Hur stor del av företagen i Sverige använder öppen källkod idag och hur stor del överväger att använda sig mer av öppen källkod?
- Finns det en koppling mellan avslöjanden kring massövervakning och intresset för öppen källkod bland svenska företag?

1.3 Avgränsningar

Eftersom det framkommit genom läckta dokument att svenska FRA samarbetar med USAs motsvarighet NSA görs en avgränsning till endast svenska företag då dessa skulle kunna vara måltavla för övervakning genom just FRA.

Här följer avgränsningarna i punktform.

- Endast svenska företag.
- Rapporten omfattar enbart en studie, inga tekniska förslag för företag kommer att presenteras.

1.4 Disposition

Det första avsnittet behandlar bakgrunden och problemformuleringen samt en redogörelse av syftet med rapporten. Avsnittet beskriver även inom vilka ramar rapporten kommer att fokuseras på.

Det andra avsnittet kommer att ge en bild av den bakomliggande teori som läsaren bör ta del av gällande öppen källkod, massövervakningen samt de avslöjanden som skett kring dess omfattning. Kapitlet tar upp viktiga avslöjanden samt Sveriges inblandning i dessa avslöjanden.

Det tredje avsnittet beskriver valda metoder som ligger till grund för rapportens genomförande. Kapitlet beskriver även tillvägagångssättet, val av litteratur samt datainsamlingen.

Det fjärde avsnittet behandlar resultatet av den empiriska studie som genomförts för att besvara frågeställningarna. En presentation av datainsamlingen i form av respondenternas svar och åsikter samt en analys av dessa svar redovisas.

Det femte avsnittet behandlar författarens tankar kring resultatet och metoden i form av en diskussion. Slutsatser baserat på den insamlade informationen i studien presenteras samt rekommendationer kring hur studien skulle kunna fortsätta och utvecklas.

2 Teoretisk bakgrund

Kapitlet behandlar den teori som ligger till grund för rapporten och är av vikt för att kunna förstå rapportens sammanhang.

2.1 Massövervakningen

2.1.1 Bakgrund

2000-talets största läckage av hemlighetsstämplade dokument skedde 2013 av amerikanen Edward Snowden, en tidigare CIA och NSA-anställd IT-konsult, numera känd som ”visselblåsaren”. Edward Snowden befinner sig i nuläget i Ryssland där han beviljats tillfällig asyl till följd av flykten från USA där han åtalats på flera punkter bl.a. stöld av statlig egendom samt oauktorerad kommunikation av försvarshemligheter. (5) (6) (7) Under loppet av 2013 läckte Snowden sammanlagt 1,7 miljoner dokument där merparten av dessa publicerats bilateralt av nyhetsorganisationer världen över, i synnerhet ”The New York Times”, brittiska ”The Guardian”, tyska ”Der Spiegel”, franska ”Le Monde” samt även ”Sveriges Television”. (8)

Nyhetsorganisationernas rapporter har särskilt belyst dokumentation som styrker de hemliga avtal som skrivits under av medlemmarna inom det så kallade UKUSA samarbetet vars avsikt är att implementera ett globalt övervakningssystem. De fem medlemsnationerna, även kallade ”The Five Eyes”, är Australien, Kanada, Nya Zeeland, Storbritannien och USA. Utöver dessa finns även andra medverkande nationer där de större europeiska nationerna, inräknat Sverige, finns representerade. (1) (9)

2.1.2 Tidslinje med betydande händelser

I maj 2013 påbörjade Edward Snowden sin påtvingade resa då han begärde tillfällig ledighet från NSA av hälsoskäl. Istället för att ”vila upp sig” reste han till Hong Kong för att träffa journalisten Glenn Greenwald samt andra representanter från den brittiska nyhetsbyrån The Guardian. (5)

I början av juni 2013 släpptes de första dokumenten som handlade bl.a. om insamlingen av amerikanska teleoperatörers telefonlistor för deras abonnenter, samt det omfattande övervakningsprogrammet PRISM, som samlar e-mail samt ljud, text och video chattar från ett okänt antal amerikanska samt utländska medborgare via företag som Microsoft, Google, Apple, Yahoo och andra stora IT-aktörer. (10) (2)

I juli 2013 samlade NSA in stora mängder information från övervakad datatrafik särskilt inriktat på Europa. Generellt samlades information in från cirka 15 miljoner telefonsamtal samt 10 miljoner internetutskick per dag. Under juli månad övervakades även EUs högkvarter i Bryssel, diplomatiska EU-anläggningar i Washington samt FNs högkvarter i New York med hjälp av utplacerade avlyssningsenheter samt infiltrerade datanätverk. (4)

Den 5 december 2013 rapporterade Sveriges Television baserat på läckta dokument att svenska FRA genomfört hemliga övervakningsoperationer med specifik fokus på Rysslands interna politik. Operationen utfördes på begäran av amerikanska NSA som mottog den data FRA samlat in. Informationsutbytet handlade även om ryska energintressen samt information om de tre baltstaterna Estland, Lettland och Litauen. (11) (12) (13) Som ett resultat av Snowdens avslöjanden kring Sveriges inblandning blev Sveriges neutralitet inom internationell politik ifrågasatt. I ett internt dokument från 2007 bekräftar NSA att relationen med Sverige är skyddad på topphemlig nivå just på grund av nationens politiska neutralitet. (14) (3) (15) Specifika detaljer kring informationsutbytet med medlemmarna av UKUSA samarbetet är följande:

- Svenska FRA har tillgång till en analysdatabas utvecklad av NSA för e-mail samt övervakning av kabelnätverk kallad Xkeyscore. (16)
- Sverige har kontinuerligt uppdaterat NSA om ändringar inom svensk lagstiftning som möjliggjort ett legalt informationsutbyte mellan svenska FRA (Försvarets Radioanstalt) och SÄPO (Säkerhetspolisen). (16)
- En NSA anställd analytiker specialiserad på antiterrorism har varit stationerad i Stockholm sedan januari 2013. (16)

Informationsutbytet med UKUSA samarbetet är dock inte begränsat till 2000-talet. Redan 1954 skrev Sverige under ett hemligt avtal tillsammans med UKUSAs medlemsnationer gällande samarbete samt utbyte av underrättelser. (14)

Hoppar vi fram i tiden till första kvartalet 2014 har inga större läckage skett kring Sveriges inblandning. Läckta dokument fortsätter dock att publiceras av nyhetsbyråer världen över specifikt detaljerande uppgifter kring i huvudsak NSAs olika övervakningsprogram och projekt.

2.1.3 Politiska reaktioner

USAs president Barack Obama försäkrade allmänheten under hösten 2013 att det inte sker någon övervakning av amerikanska medborgare. (17) Under samma tidpunkt försäkrade en politisk talesman från vita huset utländska medborgare att USA inte kan övervaka på en internationell nivå utan ett ”giltigt utländskt underrättelseändamål”. (18)

Sveriges utrikesminister Carl Bildt har även uttalat sig i frågan, där han försvarade FRA och dess projekt och beskrev dessa som ”en nationell nödvändighet” (19) Försvarsminister Karin Enström har citerats när hon uttalar sig om att Sveriges underrättelseutbyte är av avgörande betydelse för nationens säkerhet samt att underrättelseoperationer sker inom ramen för gällande lagstiftning, strikt kontroll samt under regeringens översyn. (12)

2.1.4 PRISM

PRISM är ett tidigare hemligt datautvinningsprogram för massövervakning som den amerikanska underrättelsetjänsten NSA (National Security Agency) skapade 2007. (20) PRISM har kapacitet att samla in lagrade loggar för kommunikation på internet via företag som exempelvis Microsoft och Google. I början kunde denna insamling enbart ske med tillåtelse från domstol i aktiva rättsmål. (2) Detta ändrades under 2011 då NSA genomförde en ”regeländring” vilket möjliggjorde datainsamling genom en bakdörr vilket i sin tur inte krävde tillåtelse från domstol utan kunde ske på begäran. (21)

PRISM offentliggjordes senare av Edward Snowden när han med hjälp av journalister publicerade bl.a. 41 powerpointbilder där PRISMs kapacitet och medverkande företag fanns listade. Nyhetsorganisationen The Guardian avslöjade genom dessa källor att NSA hade tillgång till chatloggar och e-mail från bl.a. Microsoft Hotmail, Skype, Yahoo och AOL. (22) (23) Flera företag vars medverkan inom PRISM avslöjats har senare uttalat sig om och försvarat sig gällande NSAs tillgång till deras servrar. (24) Internationella uttalanden har bl.a. skett från en holländsk medlem av europaparlamentet, Sophie in 't Veld som kallade PRISM för "ett direkt och medvetet brott mot EU:s lagar". (25)

2.1.5 Xkeyscore

Xkeyscore är ett tidigare hemligt övervakningsprogram utvecklat av amerikanska NSA i syfte att insamla och analysera globalt inhämtad data. Programmet används av ett flertal underrättelsetjänster världen över. (26) (27) Xkeyscore är ett komplicerat system och det finns många olika uppfattningar kring dess kapacitet. Edward Snowden beskrev Xkeyscore som ett system som möjliggör nästan obegränsad övervakning av vem som helst, var som helst i världen. NSA tillbakavisar dock detta påstående och hävdar att dess kapacitet och användning är begränsad. (26) I en tysk intervju sade Edward Snowden följande om Xkeyscore: "Du kan läsa e-mail från vem som helst i världen som innehar en e-postadress. Du kan se trafik till och från vilken webbplats som helst. Alla datorer en person använder kan du se, bärbara datorer som de övervakar kan du spåra och följa hur den rör sig från plats till plats i världen. Det är en åtkomstpunkt för samtlig information för NSA". (28) (29) (30) Som tidigare nämnts har även svenska FRA tillgång till detta system. (16)

2.2 Öppen källkod

2.2.1 Definition

När begreppet "öppen källkod" används i denna rapport följs den definition som beskrivs enligt Open Source Initiative, detta för att underlätta att tyda skillnaderna mellan öppen källkod och det som kallas "Free Software". Den största skillnaden mellan de två begreppen är att "Free Software" fokuserar mer på ideologiska aspekter kontra öppen källkod där fokus är mer praktiskt inriktat. Open Source Initiative använder tio punkter för att beskriva vad de anser att öppen källkod innebär. Det innebär inte bara att licensen ska ge tillgång till källkoden utan även en rad andra komponenter. Här följer en beskrivning av dess definition som måste följas för att en licens ska bli godkänd för att mjukvaran som licensieras under den ska få kallas öppen källkod. Detta är den beskrivning som även förklarar hur begreppet tolkas.

Licensen för produkten får inte begränsa någon att sälja den vidare eller ge bort programvaran som en del i ett större programpaket. Licensen får heller inte tillåta ägaren att ta ut en royalty avgift eller dylikt för mjukvaran då den säljs vidare eller ges bort.

Programmet måste inkludera källkod. Källkoden måste också vara tillåten att distribueras både som källkod och kompilerad form. Skulle produkten mot förmodan inte distribueras inklusive källkod måste det finnas tydliga instruktioner som talar om hur användaren hittar källkoden. Källkoden måste också gå att få tag på helt gratis eller genom ett självkostnadspris som till exempel kostnad för cd-skiva och frakt.

Licensen måste tillåta att källkoden ändras och att förgreningar av programmet skapas. Dessa ändringar och förgreningar måste också tillåtas släppas under samma licens som den ursprungliga mjukvaran.

Den licens som vill kalla sig för en öppen källkodslicens kan dock begränsa distributionen av modifierad källkod. Ett exempel är om programmet tillåter att modifieringar görs i så kallade ”patch filer” där modifieringen istället kan ske i dessa filer, vilka används tillsammans med källkoden vid kompilering för att kunna skapa modifierade versioner av programvaran. Licensen måste fortfarande tillåta distribution av mjukvara byggd på det beskrivna sättet. Licensen får dock ställa krav på att den nyutvecklade grenen av programmet måste släppas under annat namn och versionsnummer. Om en del av programvaran plockas ut ur ett programvarupaket som totalt distribueras under licensen, ska den delen kunna distribueras vidare och samma licens ska gälla för den delen som extraheras ur det totala programpaketet.

Licensen får inte under några omständigheter diskriminera någon person eller grupp i samhället. Licensen får heller inte skrivas så att ett visst område diskrimineras, till exempel förhindra användande vid viss forskning eller hos ett visst företag. Den får heller inte skrivas så att någon av de parter som programvaran distribueras till lyder under olika strikt licens utan alla som mjukvaran distribueras till ska ha samma villkor.

Om mjukvara distribueras som är licensierad under en licens godkänd av Open Source Initiative och följer dess definitioner, får licensen i fråga inte heller begränsa andra licenser. Till exempel får licensen inte begränsa andra licenser från att ta betalt om programmet distribueras som en del i ett större programpaket. Till sist måste licensen vara teknologi-neutral vilket innebär att licensen inte får begränsa användaren från att använda programvaran tillsammans med ett visst gränssnitt eller tillsammans med en viss teknologi. (31) (32)

2.2.2 Historik kring utvecklingsvägar

Traditionellt utvecklas mjukvara av ett slutet sällskap. Det gäller projekt baserade på öppen källkod liksom proprietär mjukvara. Ett slutet sällskap arbetar med källkoden och mentaliteten är generellt att det krävs djup kunskap hos de som är med och utvecklar. Eric Raymond kallar detta för katedralmodellen. (33) När Linux började utvecklas gjordes detta enligt en annan modell som Raymond kallar för basarmodellen. Skillnaden mellan basar- och katedralmodellen är synen på debugging av en mjukvara.

2.2.3 Fördelar och möjligheter med öppen källkod

När man talar om fördelar med öppen källkod kontra sluten källkod delas dessa fördelar vanligtvis upp i olika aspekter. Sett utifrån massövervakningens påverkan på IT-system är dessa fördelar något att betrakta som ett alternativ i skyddet av en IT-miljö.

2.2.3.1 Autonomi

Med i regel alla programvaror inträffar generellt någon form av systemfel under drift. Är systemet uppbyggt med öppen källkod är det upp till den egna organisationen att åtgärda detta. Fördelen är då att man inte är bunden till, och på så sätt beroende av, en extern leverantör för att lösa detta. Skulle kompetensen mot förmodan inte finnas inom organisationen för att lösa problemet, kan man söka assistans på egen hand.

2.2.3.2 Anpassningsbar programvara

När man använder sig av programvara baserad på öppen källkod får man som beskrivits tidigare fri tillgång källkoden vilket innebär friheten att modifiera och kompilera om denna efter gällande behov. Begreppet att ”skräddarsy” sin IT-miljö med den funktionalitet som organisationen behöver får en helt ny mening, vilket kan resultera i en mycket bra och unik IT-miljö som kan svårgöra övervakning från exempelvis NSAs system då dessa till stor del är anpassade till programvara baserad på slutna källkod.

2.2.3.3 Programvara med långvarig användbarhet

Projekt som baseras på användandet av öppen källkod är direkt beroende av en stark samfällighet. Finns detta kommer systemen högst troligen vara i ständig utveckling. Ett exempel på detta är Linux och operativsystemet Ubuntu som varit under ständig utveckling sedan början av 1990-talet. Denna nivå på utveckling resulterar i en programvara som kommer vara användbar under en längre tid.

2.2.3.4 Ekonomiska besparingar

På grund av att programvara med öppen källkod ofta faller under en så kallad GPL-licensering är det möjligt och ibland även vanligt förekommande att man utan kostnad kan hämta hem fullständig programvara som är färdig att användas. På så sätt kan företag och organisationer undvika dyra inköps- och licenspriser. Har programvaran en stark Community bakom sig underlättar även detta underhåll och framtida uppdateringar.

2.2.4 Nackdelar och risker med öppen källkod

En nackdel som kan vara problematisk är att de flesta företag och organisationer har en befintlig samling sammankopplade system som man isåfall måste ta hänsyn till vid integration av programvara med öppen källkod i befintlig IT-miljö. Detta leder i sin tur till att trots att programvaran i sig kan vara gratis, kan integrationen medföra dyra utgifter. Det är därför viktigt att man även tar i beräkning integrationskostnader och inte blir lurad av ”gratis programvara”. En annan risk med dessa produkter är att det ofta ställs nya krav på användarna, krav som organisationen möjligtvis inte kan hantera då deras anställda inte har den tekniska kompetens som behövs för att kunna använda produkten. Detta gäller självklart inte alla system med öppen källkod, dock betraktas tröskeln högre vad gäller teknisk kunskap. (34)

3 Metod och genomförande

Kapitlet beskriver den valda metoden för genomförandet av arbetet samt tillvägagångssättet som ligger till grund för resultatet.

3.1 Metodval och tillvägagångssätt

För att besvara mina frågeställningar har en empirisk studie genomförts baserat på insamlandet av företags och organisationers åsikter kring massövervakningen samt deras syn på öppen källkod och om det finns en möjlig koppling mellan de två koncepten. Vid insamling av primärdata har en kvalitativ metod valts i syfte att skapa en djupare förståelse för vad som kan ligga bakom de slutsatser som kommer dras från studien. Eftersom man inte i förväg kunde avgöra vad som var bakomliggande faktorer till de primärdata som insamlats, var ett öppet förhållningssätt till den insamlade datan att föredra. (35)

För att samla in primärdata till studien genomfördes semistrukturerade intervjuer. I det inledande stadiet planerades säljare på rikstäckande IT-företag att intervjuas. Med IT-företag menas företag vars mål är att förse sina kunder med teknikstöd för deras verksamhet. Detta på grund av att dessa säljare har kontakt med kunder i flera olika branscher, bland annat IT-tekniker och beslutsfattare på olika nivåer vilket borde ge en god bredd på innehållet i den insamlade datan. Berörda personer att intervjuas var också personer med god insikt, både internt mot företaget samt externt ut mot dess kunder. Bedömningen var att de ser och hör mycket och har en viss insikt i hur trenden ser ut gällande efterfrågan på öppen källkod från kund och hur tekniker och beslutsfattare ställer sig till konceptet.

Vid intervjutillfällena planerades en intervjuguide att användas med ett antal frågor, samtidigt som intervjuerna hölls så öppna som möjligt för att få fram variation och inte styra den information som uppgiftslämnaren tillhandahöll. På grund av begränsad tidsåtgång planerades studien innehålla någonstans mellan fyra och sex intervjuer. Intervjuerna planerades även att bandas i syfte att underlätta en efterföljande transkribering och analys av intervjumaterialet.

3.2 Val av litteratur

Inledningsvis togs underlag och litteratur fram för att styrka bakgrunden. Därefter undersöktes material som kunde påvisa det generella intresset för öppen källkod historiskt och fram till idag. Litteratursökningen innefattade även material som kan styrka de avslöjanden som skett kring massövervakningen, både internationellt och nationellt. Speciellt intresse fanns även för att hitta litteratur som kunde hjälpa till att tolka och finna samband hos primärdatan som samlades in under studien. Sådant material skulle vara både kvantitativa och kvalitativa undersökningar kring intresset för öppen källkod i framför allt Sverige men även studier som genomförts i andra länder eller globalt. Undersökningar som även pekade på anledningar till varför öppen källkod blir mer eller mindre populärt hos företagen var också av intresse. Dessa typer av studier tänktes kunna påvisa eller förtydliga samband, olikheter eller trender avseende intresset för öppen källkod.

3.3 Datainsamling och analys

När primärdata och sekundärdata hade samlats in genom intervjuer skedde en sammanställning och analys. Sammanställningen inkluderade renskrivning av rådata, transkribering av ljudinspelningar samt sammandrag av all information som samlats in genom intervjuerna. Därefter genomfördes en analys baserat på svaren från intervjuerna vilket ledde fram till ett resultat. Resultatet kopplades mot den information kring massövervakningen som offentliggjorts och som fortsätter offentliggöras. Resultatet skulle då kunna peka på om det finns generella tendenser åt att intresset för öppen källkod har förändrats eller att det helt enkelt inte har påverkats som en följd av övervakningsskandalerna. Skulle det inträffa att inga tendenser kunde urskiljas skulle bredden på svaren som intervjuerna tillhandahåller potentiellt kunna påvisa varför övervakningsskandalerna inte har påverkat intresset. Intervjuguiden som användes under intervjuerna är designad till att ge respondenten en chans att först presentera företaget för att sedan gå in på frågor kring ämnet. Ämnesfrågorna är designade utifrån syftet och de två frågeställningarna. Frågorna är även utformade till att framhäva öppenhet och mer fria svar eftersom ämnet är relativt brett och respondenternas åsikter beskriva med deras egna ord är viktiga för studien.

4 Resultat och analys

Kapitlet behandlar resultatet av studien med utgångspunkt från respondenternas svar samt svaren på ställda frågeställningar genom en analys av dessa.

4.1 Respondenternas svar och åsikter

Totalt har fem företag intervjuats, tre intervjuer skedde på plats hos företaget i fråga och två intervjuer skedde via mail samt skype på grund av att respondenten befann sig på annan ort vid intervjutillfället. Svaren från dessa två respondenter är därför något mer kortfattade jämfört med de första tre. Företagen benämns i resultatet som ”Respondent 1 – 5”. För att presentera respondenternas svar, åsikter, tankar och resonemang kring ämnet kommer frågorna från de genomförda intervjuerna delas upp i fem kategorier; En presentation av företaget/organisationen, uppfattningen om massövervakningen och dess påverkan, uppfattningen om, samt i vilken utsträckning företaget idag använder sig av öppen källkod, synen på säkerheten i tjänsteleveranser till kund samt synen på en koppling mellan massövervakning och öppen källkod.

4.1.1 Presentation av respektive respondent

I och med att rapporten skall vara generell är det viktigt att tillhandahålla en kort presentation av respektive respondent i syfte att påvisa ett brett urval vad beträffar branschriktning och företagsstorlek.

Respondent 1 är ett litet företag med ett fåtal anställda med bas i Jönköping. Företaget är en tjänsteleverantör inom datacenter, infrastruktur och säkerhet där de valt att arbeta enbart med produkter inom öppen källkod.

Respondent 2 är ett mindre företag med ett tiotal anställda med bas i Jönköping. Företaget är en produkt/tjänsteutvecklare inom RFID (Radio Frequency Identification). Företaget levererar RFID lösningar till bl.a. transport och logistikbranschen för att underlätta hanteringen av gods.

Respondent 3 är ett större internationellt bolag med huvudkontor i Jönköping med kontor på andra platser i Sverige. Företaget är en IT-tjänsteleverantör specialiserat på mjukvaruutveckling där de levererar lösningar till både andra IT-företag samt offentlig sektor.

Respondent 4 är ett större nordiskt bolag med huvudkontor i Stockholm och kontor i Jönköping. Företaget är en IT-tjänsteleverantör inom drift, outsourcing, applikationsutveckling och säkerhet. Företaget levererar IT-tjänster till Sveriges största företag och organisationer.

Respondent 5 är ett större nordiskt bolag med internationella kontakter. Företaget är en IT-tjänsteleverantör inom applikationshantering, systemutveckling och försvarssystem. Företaget arbetar även med mobila lösningar och E-handel.

4.1.2 Uppfattning om massövervakning och dess påverkan

Då det är av stor vikt för studien att ta reda på svenska företags uppfattning och synsätt på massövervakningen och dess påverkan/inverkan, frågades respondenterna om detta.

Respondent 1 svarade att han anser att det är nyttigt att det framkommit information kring massövervakning så att folk nu får upp ögonen för övervakningen. Han uttalar sig även om att han tycker det är fruktansvärt att övervakningen är så pass global och inkräktande och att vi inte riktigt förstår ännu vad detta kan leda till i längden. Han uttrycker att som företag har de påverkats något positivt då diskussioner börja träda fram kring var information lagras. Han säger att de har fått många förfrågningar från större företag, särskilt företag som arbetar med media, att de är noggranna med att information ska skyddas med PUL (Personuppgiftslagen) samt att informationen lagras inom Sverige och att den är säkrad från obehörig åtkomst. Han antar även att företagen som hört av sig har blivit mer uppmärksamma inom området från bl.a. diskussioner och från nyheter och media. Företag vill säkerställa att de inte blir utsatta, avslutar han med.

Respondent 2 svarade att han och företaget har blivit mer försiktiga kring hur de hanterar digital information som de sparar eller skickar. Han förklarar vidare med att digitalt sparad information känns offentlig och att det är en känsla samt en oro företaget idag har till följd av massövervakningen. Han nämner också att företaget undviker till största delen det är möjligt tjänster i molnet för deras företagskänsliga information samt att de nyligen reviderat sin IT-säkerhetspolicy med nya riktlinjer kring hantering av känsliga företagsfiler. Respondent 2 nämnde även att han privat i viss mån undviker att spara information på datorn utan använder sig då istället av papperskopior. Respondent 2 berättade även att han tror att på sikt kommer informationshantering bli mer strikt samt att förhållningsättet kommer förändras inom företag och organisationer. Han berättade även vidare att när massövervakningen offentliggjordes under 2013 blev detta som en bekräftelse på något de länge anat.

Respondent 3 anser att massövervakningen påverkar branschen samt att förhållningsättet mot IT-säkerhet kommer förändras till följd av vad som offentliggjorts. Respondenten tycker också att det är positivt att massövervakningen bidragit till att företag lägger större fokus på frågor gällande insyn samt ser över hanteringen av till exempel dokument av möjlig företagskänslig natur. Respondenten ger också tekniska exempel kopplade till avslöjandet kring stora IT-företags medverkan i övervakningsprogrammet PRISM, företag som Google och Dropbox vars tjänster används flitigt inom flertalet svenska företag. Respondenten påpekar att tjänster som Google Apps för företag samt Dropbox finns väl representerat inom svenska företag och att detta skapar problem ur en säkerhetssynpunkt. Respondenten nämner dock att hans företag inte använder sig av dessa tjänster och att företaget nyligen reviderat sin IT-säkerhetspolicy till följd av offentliggörandet av massövervakningen.

Respondent 4 anser att massövervakningen påverkar branschen samt att synen på IT-säkerhet inom företag kommer att förändras. Respondenten nämner att massövervakningen lett till att företaget ändrat sin IT-säkerhetspolicy om hur hanteringen av känsliga filer och dokument ska ske. Vidare berättar respondenten att som företag har de inte tillämpat några större åtgärder inom sina IT-miljöer, men att frågan har varit aktuell vid möten och sammanträden och att inga större ändringar finns inplanerade för företaget i nuläget.

Respondent 5 svarade att företaget blivit försiktigare med hur de hanterar digital information samt att de genomfört förändringsplaner för hur denna hantering skall gå till. IT-säkerhetspolicyn har även blivit reviderad till följd av massövervakningen. Respondenten uttryckte att företaget tar massövervakningen på stort allvar och planerar att genomföra ytterligare åtgärder gällande säkerhet utan att nämna några tekniska förslag.

4.1.3 Uppfattning om öppen källkod samt uppskattad användning

Då det är av stor vikt för studien att ta reda på svenska företags uppfattning om öppen källkod samt i vilken utsträckning de idag använder sig av programvara och system med öppen källkod, frågades respondenterna om detta.

Respondent 1 förklarar att han tycker det är ett bra sätt att bygga applikationer och att det ur ensäkerhetsynpunkt inte går att dölja något för användaren på samma sätt som i slutna källkod. Han berättar även att de har byggt hela sin verksamhet runt just öppen källkod. Samtidigt tycker han att det är fenomenalt att många unga hoppar på projekt med öppen källkod där de lär sig att koda och utveckla. Han påpekar också att studenter och unga idag i genomsnitt har högre och bredare kunskap än för fem till tio år sedan vilket han anser är tack vare öppen källkod och det ökande intresset inom området. Vidare tar han upp att han tror att det finns två läger inom företagsvärlden när det kommer till öppen källkod; de som bryr sig mycket om licenspengarna och ser en besparing i öppen källkod samt de som ser öppen källkod som en alternativ väg, rentav en bättre väg att sätta upp system på. Öppen källkod har blivit ett mer accepterat alternativ, särskilt när man tittar på företag som Facebook och Google som använder sig mycket av öppen källkod där det visat sig vara stabilt, robust och fungerar i praktiken. Respondentens uppfattning är att betydelsen av öppen källkod ökat sedan massövervakningen avslöjats. Vid frågan om företagets användning av öppen källkod svarar respondenten att de använder sig av öppen källkod i så stor skala som möjligt. Han uttalar sig även om att de byggt sin hostinglösning enbart med öppen källkod. Respondenten säger även att han tror att man idag kan ersätta samtliga system inom en IT-miljö med öppen källkod om man skulle vilja och om man är beredd att ta den extra kostnaden integrationen/implementeringen isåfall skulle innebära. Företaget använder sig idag av öppen källkod i 90 % av samtliga tjänster.

Respondent 2 svarar att företaget idag använder sig av vissa tjänster baserade på öppen källkod. Respondent 2 förklarade att tack vare branschen som företaget agerar inom, samt att de inte är en direkt tjänsteleverantör utan istället levererar produkter med egenutvecklad mjukvara, detta bidrar till att de inte funderat på alternativa programvaror inom exempelvis kontoret utan detta är mera experimentellt. Företaget planerar dock att erbjuda sina lösningar med stöd för öppen källkod i framtiden.

Respondent 3 nämner att företaget arbetar med både slutna och öppen källkod. Öppen källkod är starkt representerat hos företaget då de arbetar mycket med mjukvaruutveckling inom exempelvis Java samt att de starkt förespråkar programvara baserad på öppen källkod både inom företag samt gentemot kund. Respondenten nämner också att merparten av de anställda utvecklar programvaror med öppen källkod samt att medverkan inom öppen källkods-samfälligheten är väl representerad. Respondenten nämner att tjänster med öppen källkod gentemot kund är starkt representerad samt att användandeutsträckningen sannolikt kommer förändras ytterligare, dels till följd av massövervakningen med också utifrån ett ökat intresse inom branschen.

Respondent 4 nämner att företaget i stort sett arbetar med proprietär mjukvara och att de innehar en utpräglad Microsoft-miljö. Respondenten nämner att hans personliga åsikt är att öppen källkod har blivit ett mer accepterat lösningsförslag inom branschen men att detta inte är något det egna företaget har någon plan på att implementera.

Respondent 5 svarar att företaget arbetar med både sluten och öppen källkod. Företaget använder sig särskilt mycket av öppen källkod inom mjukvaruutveckling vilket representerar en relativt stor del av företagets tjänstekatalog. Respondenten nämner att företaget anser öppen källkod som ett bra och alternativt sätt att bygga applikationer på. Respondenten nämner även att efterfrågan på system och applikationsstöd för öppen källkod har ökat från kunder och inom branschen, vilket enligt respondenten påvisar att öppen källkod numera ses som ett mer accepterat alternativ inom IT.

4.1.4 Säkerhetssyn på tjänsteleverans

Säkerhet är ett intressant ämne till följd av massövervakningen, särskilt med tanke på stora IT-aktörers informationsutbyte med NSA. Respondenterna utfrågades om deras syn på informationssäkerhet och hur de garanterar sina kunders säkerhet inom tjänsteleveransen.

Respondent 1 förklarar att de i nuläget inte har en förändrad säkerhetssyn sedan massövervakningen blev allmänt känd utan istället har fokuserat på att förbättra och bygga vidare på sin IT-säkerhetspolicy samt att de sett över sina system och krypteringshantering.

Respondent 2 förklarar att deras produkter i stort sätt kommunicerar på slutna nätverk med hjälp av radiolänk där de i nuläget har bestämt sig för att kryptera informationen, i viss mån till följd av massövervakningen. Respondent 2 berättar vidare att de just nu håller på med en process för att deras system ska bli certifierat vilket har lett till att de ser över existerande tjänster och hanteringen av dessa samt om förbättringar kan tillämpas. Detta utifrån ett intresse att kika på alternativa mjukvaror och lösningar.

Respondent 3 nämner att företaget har flera bankkunder och att de anser att det främst är erfarenhet och beprövad teknik som är viktigt i deras säkerhetsanalys kring levererade tjänster. Vidare nämner respondenten att de har tillit till sina leverantörer men att de också alltid strävar efter att bygga system på ett så robust och säkerhetsmässigt sätt de kan. Respondenten nämner även att de flesta säkerhetshål beror på den mänskliga faktorn och inte till följd av ”fel” hos programvaran.

Respondent 4 förklarar att företaget har som rutin att genomföra säkerhetskontroller av sina tjänsteleveranser enligt checklista och utefter schema. Företaget genomför också ett moment de kallar ”Omvärldsbevakning” vilket innebär kontroller av säkerhetsuppdateringar från bl.a. Symantec samt kontroller om dessa kan tillämpas på deras system. Respondenten nämner att företaget har tillit till sina leverantörer men att de också genomför egna kontroller innan tjänsteleverans till kund.

Respondent 5 svarar att företaget planerar att utöka sin användning av alternativ programvara inom öppen källkod då företaget har en gemensam syn på öppen källkod som ett säkrare och mer kontrollerbart alternativ. Respondenten förklarar att i dagsläget håller sig företaget uppdaterat i förhållande till nyheter inom säkerhet och att de tillämpar säkerhet som en av de viktigaste, om inte den viktigaste kvalitén inom sina tjänsteleveranser.

4.1.5 Koppling mellan massövervakning och öppen källkod

Den avslutande kategorin av intervjufrågor tar upp huvudfrågan i studien nämligen om respondenterna anser att det finns en koppling mellan massövervakningen och intresset för öppen källkod sett utifrån ett säkerhetsperspektiv, omnämnt i föregående kategori, som ett eventuellt skydd mot övervakning och insyn.

Respondent 1 anser att öppen källkod kommer att få ett starkare fäste som ett ännu mer accepterat alternativ då flera stora företag börjar titta på lösningar med öppen källkod. Att det ökade intresset är en följd av massövervakningen kunde respondenten inte uttala sig om. Dock tror han att öppen källkod är framtiden för utveckling och säkerhet. Respondenten nämnde dock att han tror att det kan finnas en koppling mellan öppen källkod och massövervakningen sett utifrån ett synsätt att många som är passionerade för öppen källkod även brinner för yttrandefrihet och pressfrihet samt har lagt mycket politiska och ideologiska värderingar till praktiken runt öppen källkod.

Respondenten anser också att han inte tror marknaden och slutanvändarna är tillräckligt insatta för att förstå magnituden av problemet i dagsläget men att det säkerligen kommer att ändras med tiden. Han anser även att tilliten till leverantörer som Microsoft, Google, Apple, Yahoo och Skype kommer minska då avslöjanden har skett som visar på att dessa företag delar kunduppgifter med NSA. Han är övertygad om att debatten kommer att intensifieras under de kommande åren.

Respondent 2 kände att han inte kunde ge ett direkt svar på om det finns en koppling men att han anser, och tror, att alternativa lösningar med exempelvis öppen källkod är av intresse för svenska företag, särskilt utifrån ett säkerhetsperspektiv. Respondent 2 tror också att massövervakningens påverkan ännu inte riktigt fått genomslag hos svenska företag men att detta kommer ändras längre fram. Respondent 2 tryckte även på att han och företaget ser säkerhet som en viktig kvalitet, särskilt vid informationsutbyte mellan företag och kund men också internt informationsutbyte av exempelvis känsliga filer.

Respondent 3 tror att intresset för öppen källkod ökat inom samfälligheten. Respondenten tror att företag, som exempelvis har en utpräglad Microsoft-strategi, innehar ett generellt svalt intresse till att se över sin IT-miljö genom att introducera alternativa system och programvaror. Respondenten tror att den bidragande faktorn till det ökade intresset för öppen källkod hos dessa företag i så fall mynnar ut i frågor om licenskostnader. Respondenten tror inte att ett ökat intresse av öppen källkod idag är till följd av massövervakningen eller att det anses som ett säkrare alternativ. För etablerade företag med proprietärt inriktad mjukvara är det enbart ett intressant alternativ utifrån en kostnadssynpunkt. Vidare nämner respondenten att han tror att merparten av branschen ännu ej är benägna att förändra sina IT-miljöer till följd av massövervakningen, då de antingen inte ser det som ett hot/problem eller att de rentav inte är insatta i vad massövervakningen innebär.

Respondenten påpekar dock att detta kanske inte är fallet inom statlig verksamhet då de ofta har andra åsikter kring insyn och säkerhet. Respondenten är också kritisk till att de företag som innehar exempelvis en starkt utpräglad Microsoftmiljö inte är mer öppna för frågan kring alternativ som öppen källkod, samt att de borde vara mer kritiska mot sina leverantörer och begära in svar på deras inblandning i massövervakningen, leverantörer som Microsoft, Google och Apple vars inblandning inom PRISM avslöjats.

Respondent 4 förklarar att eftersom företaget har en utpräglad Microsoft-strategi, och därför inte arbetar med öppen källkod inom sina tjänsteleveranser, har han inte någon direkt uppfattning om det skulle kunna finnas en koppling mellan öppen källkod och massövervakningen. Respondenten nämner dock att han tror att massövervakningen bidragit till att företag ser över sina systems säkerhet men att branschen i stort ännu inte är redo för drastiska förändringar baserade på vad som offentliggjorts.

Respondent 5 anser att det säkerligen finns en koppling mellan massövervakningen och ett ökat intresse för öppen källkod och alternativa programvaror, sett utifrån de avslöjanden som skett kring stora proprietära IT-aktörers informationsutbyte med amerikanska NSA. Respondenten nämner dock att han tror att genomslagskraften gällande en förändring kommer vara långsam inom branschen då det ofta handlar om kostnadsfrågor relaterat till implementeringen. Respondenten nämner också att företag troligen kommer att bli mer medvetna vad gäller digital information och hur den skall hanteras samt att synsättet på säkerhet kommer att förändras med tiden.

4.2 Analys

Inledningsvis är det viktigt att påpeka att efter de genomförda intervjuerna med respondenterna, anser författaren till denna rapport att det känns som att de olika respondenterna haft en relativt enad syn på massövervakningen och dess effekter på IT-branschen. Synen på öppen källkod är dock mer spridd mellan respondenterna, något man kan anse vara mer förståeligt då inte samtliga företag arbetar med öppen källkod. För att förtydliga likheterna samt olikheterna mellan respondenternas svar och åsikter kommer författaren presentera en sammanfattad vy utifrån de olika specificerade kategorierna.

4.2.1 Uppfattning om massövervakning och dess påverkan

Merparten av respondenterna anser att massövervakningen påverkar branschen och att synen på säkerhet kommer att förändras på grund av de avslöjanden som skett. Flera av respondenterna nämner även att de förändrat sina IT-säkerhetspolicys framför allt, hur de ändrat hanteringen av dokument och uppgifter efter det att massövervakningen offentliggjorts. Generellt verkar det också som att svenska företag ännu inte är särskilt insatta i massövervakningen och vad som inträffat utan att den information de besitter har varit begränsad till nyheter och inte utav efterforskning på eget intresse. Sensmoralen verkar vara att massövervakningen inte riktigt fått ett genomslag där företag ser förändringar som akut nödvändiga utan fokus verkar istället ligga på reviderade IT-säkerhetspolicys samt en ökad försiktighet i hanteringen av digital information.

4.2.2 Uppfattning om öppen källkod samt uppskattad användning

Två av respondenterna svarar unisont med att de anser att öppen källkod är ett bra sätt att bygga applikationer på. Merparten av respondenterna arbetar med öppen källkod inom sina tjänster och samtliga anser att öppen källkod har blivit ett mer accepterat alternativ inom branschen. Två av respondenterna nämner även att efterfrågan på stöd för öppen källkod ökat från kund samt att intresset för öppen källkod verkar ha ökat inom branschen under det gångna året.

4.2.3 Säkerhetssyn på tjänsteleverans

Merparten av respondenterna svarar att de genomför ändringar inom säkerhetspolicyn samt att man är generellt mer försiktig med hur man hanterar filer. Två av respondenterna svarar att de har tillit till sina leverantörer och att de håller sig uppdaterade vad avser nyheter inom säkerhet. En respondent anser även att de flesta säkerhetshål är mänskliga och inte till följd av ”fel” hos programvara.

4.2.4 Koppling mellan massövervakning och öppen källkod

Merparten av respondenterna är eniga om att de anser att massövervakningen har varit en starkt bidragande faktor till en förändrad syn på säkerhet, samt att det lett till att företag tittar på alternativa lösningar till att skydda mot otillbörlig insyn. Merparten av respondenterna anser att öppen källkod troligen kommer bli ett ännu mer accepterat alternativ efter offentliggörandet av övervakningsprogrammet PRISM. Flera respondenter nämner även att genomslagskraften ännu ej varit betydande och att branschen inte är redo för större förändringar, utan begränsar sig istället till att förändra sin IT-säkerhetspolicy samt öka kraven kring hantering av dokument och filer.

5 Diskussion och slutsatser

Kapitlet behandlar författarens diskussion och reflektion över resultatet, metoden samt slutsatsen av studien.

5.1 Resultatdiskussion

När denna studie påbörjades ställde jag följande frågeställningar:

- *Hur stor del av företagen i Sverige använder öppen källkod idag och hur stor del överväger att använda sig mer av öppen källkod?*
- *Finns det en koppling mellan avslöjanden kring massövervakning och intresset för öppen källkod bland svenska företag?*

Efter att jag inledningsvis fördjupat mig inom aktuell litteratur och artiklar kopplade till ämnet, samt genomfört datainsamlingen utifrån en kvalitativ metod, anser jag mig inneha tillräckligt med underlag för att kunna besvara dessa frågeställningar. Baserat på genomförda intervjuer med slumpmässigt utvalda IT-företag pekar resultatet på att öppen källkod blir mer representativt för företag inom IT-branschen. Öppen källkod ses som ett mer accepterat alternativ och flertalet IT-företag använder sig idag av öppen källkod i olika utsträckning.

Vissa företag dock är inte särskilt drivande vad gäller öppen källkod. Detta visar sig gälla särskilt för större företag med exempelvis en redan inriktad och utpräglad Microsoft-strategi. Dessa företag tenderar att inte söka sig mot öppen källkod, trots att mjukvaran är gratis, eftersom det skulle kosta för mycket i implementeringskostnad. Resultatet pekar också på att intresset generellt ökar för öppen källkod och av de företag och respondenter jag intervjuade svarade flera att de planerar att utöka sitt arbete med öppen källkod och att inkludera detta mer i deras tjänsteleveranser. Flertalet företag nämner även att förfrågningar gällande öppen källkod från kund generellt ökat på senare tid.

Svenska företags generella syn på massövervakningen är att de anser att branschen har påverkats och att synen på säkerhet förändrats sedan massövervakningen offentliggjordes. Jag blev själv något förvånad över att företagen inte var lika insatta i vad massövervakningen innebär och vad exempelvis NSA är kapabla till. Sensmoralen verkar vara att frågan varit representativ inom de flesta organisationer men att man inte valt att vidta några omedelbara åtgärder. De åtgärder som genomförts av svenska företag generellt är förändringar inom IT-säkerhetspolicys samt ökad försiktighet i hanteringen av dokument och hur de sparas och skickas. Merparten av företagen hade inte en klar uppfattning om parallellen mellan massövervakningen och ett ökat intresse för öppen källkod, vilket jag fick förklara ytterligare under intervjuerna då jag tryckte på avslöjandet om PRISM och de stora IT-aktörernas medverkan. Sambandet blev senare mer klart och de företag med en mer utpräglad IT-miljö med öppen källkod uttryckte ytterligare behovet av att kunna skraddarsy sina system då detta generellt försvårar otillbörlig insyn genom övervakningsprogram som PRISM och Xkeyscore.

5.2 Metoddiskussion

Efter efterforskning bestämde jag mig för att en kvalitativ metod med semistrukturerade intervjuer var den metod som skulle passa bäst för denna typ av studie. Jag inledde min studie med att utforma en presentationstext kring mig själv och vad min undersökning gick ut på. Denna text samt ett dokument med intervjufrågor mailade jag ut till företag och berörda personer vid dessa företag. Sammanlagt mailade jag c:a 25 företag och förväntade svar från åtminstone hälften av dessa. Detta visade sig dock vara högt räknat då jag enbart fick ett fåtal svar under de första veckorna. De företag jag inte fick kontakt med ringde jag till och beskrev mitt intresse och att deras medverkan var viktig för studien. Jag genomförde mina tre första intervjuer under denna tid och de återstående två medverkande tog avsevärt längre tid att få tag på och planera in. De två sista intervjuerna genomfördes en tid senare via mailkorrespondans samt över telefon och skype. Detta på grund av att respondenterna ifråga inte kunde träffa mig personligen då de befann sig på annan ort. Detta var något jag själv inte hade väntat mig och därför blev datainsamlingen något lidande utifrån en tidsaspekt.

Att genomföra intervjuerna på detta sätt gör det svårare för respondenten, enligt min åsikt, att ge mer utstuderade svar samt att flika in intressanta sidospår vilket kan gynna konversationen. Nackdelen med att genomföra de två sista intervjuerna via mail och telefon var att respondenternas svar blev något korta jämfört med de intervjuer som skedde öga-mot-öga. Inledningsvis var tanken att intervjua mellan fyra och sex företag, vilket visade sig vara väl avvägt då tiden var begränsad och respondenternas svar var så pass utförliga att jag bedömde det som tillräckligt för studien. Jag tycker även att mitt urval blev lyckat då respondenterna hade olika synsätt på både massövervakningen och öppen källkod vilket ledde till variation och intressanta åsikter från respondenterna vilket gynnade studien.

5.3 Slutsatser och rekommendationer

Studien visar på att massövervakningen lett till ett förändrat synsätt på säkerhet hos svenska företag. Företagen har blivit mer försiktiga kring hur de hanterar sin digitala information och hur denna sparas och skickas.

Studien visar även på att öppen källkod har blivit mer representativt och accepterat inom IT-branschen. Företag använder sig av öppen källkod inom sina tjänster i större skala och massövervakningen har lett till att företag i viss mån väljer att söka sig till alternativa programvaror och system för sina IT-miljöer. Intresset för öppen källkod förväntas öka, trots att marknaden i viss mån inte ännu är mogen för större förändringar till följd av massövervakningen.

Min rekommendation är att denna studie bör upprepas inom c:a ett (1) år för att belysa eventuella skillnader som kan ha inträffat i företag och deras syn på massövervakningen då offentliggöranden kring massövervakningen fortlöpande sker.

6 Referenser

1. **Electronic Frontier Foundation.** NSA Primary Sources . *EFF*. [Online] 2013. [Citat: den 22 04 2014.] <https://www.eff.org/nsa-spying/nsadocs>.
2. **The Washington Post.** U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. [Online] den 6 June 2013. [Citat: den 8 May 2014.] http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.
3. **NSA/CSS.** Cryptome. [Online] den 18 April 2013. [Citat: den 18 02 2014.] <http://cryptome.org/2013/12/nsa-se-spies.pdf>.
4. **Der Spiegel.** Cover Story: How the NSA Targets Germany and Europe. *Der Spiegel*. [Online] den 1 July 2013. [Citat: den 2 May 2014.] <http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html>.
5. **The Guardian.** Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*. [Online] den 10 June 2013. [Citat: den 4 May 2014.] <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.
6. **The Washington Post.** U.S. vs. Edward J. Snowden criminal complaint. *The Washington Post*. [Online] den 6 June 2013. [Citat: den 8 May 2014.] <http://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/>.
7. **The New York Times.** Leaker Files for Asylum to Remain in Russia. *The New York Times*. [Online] den 16 July 2013. [Citat: den 10 May 2014.] http://www.nytimes.com/2013/07/17/world/europe/snowden-submits-application-for-asylum-in-russia.html?_r=0.
8. **Bloomberg.** Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers. *Bloomberg*. [Online] den 10 January 2014. [Citat: den 6 May 2014.] <http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html>.
9. **Electrospaces.** Five Eyes, 9-Eyes and many more. *Top Level Telecommunications*. [Online] den 22 January 2014. [Citat: den 7 May 2014.] <http://electrospaces.blogspot.se/2013/11/five-eyes-9-eyes-and-many-more.html#cfbl-network>.
10. **The Guardian.** NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. [Online] den 6 June 2013. [Citat: den 5 May 2014.] <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.
11. **Sveriges Television (SVT).** Snowden files reveal Swedish-American surveillance of Russia. *Uppdrag Granskning*. [Online] den 5 December 2013. [Citat: den 6 May 2014.] <http://www.svt.se/ug/snowden-files-reveale-swedish-american-surveillance-of-russia>.
12. **Sydsvenskan.** FRA spionerar på Ryssland åt USA. *Sydsvenskan*. [Online] den 5 December 2013. [Citat: den 4 May 2014.] <http://www.sydsvenskan.se/sverige/fra-spionerar-pa-ryssland-at-usa/>.
13. **Sveriges Television (SVT).** FRA spying on “energy” and “Baltics” for USA. *Uppdrag Granskning*. [Online] den 7 December 2013. [Citat: den 5 May 2014.] <http://www.svt.se/ug/fra-spying-on-energy-and-baltics-for-usa>.

14. —. NSA "asking for" specific exchanges from FRA - Secret treaty since 1954. *Uppdrag Granskning*. [Online] den 8 December 2013. [Citat: den 7 May 2014.] <http://www.svt.se/ug/nsafra4>.
15. **The Local**. Cold War treaty confirms Sweden was not neutral. *The Local, Sweden*. [Online] den 9 December 2013. [Citat: den 10 May 2014.] <http://www.thelocal.se/20131209/secret-cold-war-treaty-confirms-sweden-was-never-neutral>.
16. **Sveriges Television (SVT)**. Read the Snowden Documents From the NSA. *Uppdrag Granskning*. [Online] den 11 December 2013. [Citat: den 6 March 2014.] <http://www.svt.se/ug/read-the-snowden-documents-from-the-nsa>.
17. **MSNBC**. Obama says 'there is no spying on Americans,' but what about our data? *MSNBC*. [Online] den 13 September 2013. [Citat: den 4 May 2014.] <http://www.msnbc.com/msnbc/obama-says-there-no-spying-americans>.
18. **The White House**. Press Briefing by Press Secretary Jay Carney, 6/13/2013. *whitehouse.gov*. [Online] den 6 June 2013. [Citat: den 4 May 2014.] <http://www.whitehouse.gov/the-press-office/2013/06/13/press-briefing-press-secretary-jay-carney-6132013>.
19. **Sveriges Radio (SR)**. Carl Bildt defends FRA surveillance as 'necessary'. *Sveriges Radio (SR)*. [Online] den 13 December 2013. [Citat: den 4 May 2014.] <http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5733081>.
20. **The Guardian**. NSA monitored calls of 35 world leaders after US official handed over contacts. *The Guardian*. [Online] den 25 October 2013. [Citat: den 10 May 2014.] <http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>.
21. —. NSA performed warrantless searches on Americans' calls and emails – Clapper. *The Guardian*. [Online] den 1 April 2014. [Citat: den 8 May 2014.] <http://www.theguardian.com/world/2014/apr/01/nsa-surveillance-loop-hole-americans-data>.
22. **The Washington Post**. NSA slides explain the PRISM data-collection program. *The Washington Post*. [Online] den 10 July 2013. [Citat: den 8 May 2014.] <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>.
23. **RT**. Microsoft helped the NSA bypass encryption, new Snowden leak reveals. *RT*. [Online] den 11 July 2013. [Citat: den 8 May 2014.] <http://rt.com/usa/microsoft-nsa-snowden-leak-971/>.
24. **Techcrunch**. Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program. *Techcrunch*. [Online] den 6 June 2013. [Citat: den 8 May 2014.] <http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/>.
25. **The Daily Dot**. Does the NSA's PRISM spying program violate EU law? *The Daily Dot*. [Online] den 7 June 2013. [Citat: den 9 May 2014.] <http://www.dailydot.com/news/prism-nsa-government-surveillance-europe-law/>.
26. **The Guardian**. The NSA is turning the internet into a total surveillance system. *The Guardian*. [Online] den 11 August 2013. [Citat: den 5 May 2014.] <http://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email>.
27. —. How the NSA is still harvesting your online data. *The Guardian*. [Online] den 27 June 2013. [Citat: den 11 May 2014.] <http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection>.
28. **NDR**. Snowden-Interview: Transcript. *ndr.de*. [Online] den 26 January 2014. [Citat: den 11 May 2014.] http://www.ndr.de/ratgeber/netzwelt/snowden277_page-3.html.

29. **The Washinhton Post.** Edward Snowden, after months of NSA revelations, says his mission's accomplished. *The Washington Post*. [Online] den 24 December 2013. [Citat: den 6 May 2014.] http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.
30. **The Guardian.** XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. *The Guardian*. [Online] den 31 July 2013. [Citat: den 11 May 2014.] <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>.
31. **Initiative, Open Source.** The Open Source Definition. *Open Source Initiative*. [Online] [Citat: den 18 February 2014.] <http://opensource.org/osd>.
32. **Creative Commons.** About The Licenses. *Creative Commons*. [Online] [Citat: den 11 May 2014.] <http://creativecommons.org/licenses/>.
33. **Raymond, Eric S.** *The Cathedral and the Bazaar*. u.o. : O'Reilly Media, 1999. 1-565-92724-9.
34. **Stefano Comino, Fabio M. Manenti.** Open Source vs Closed Source Software: Public Policies in the Software Market. [Online] 2003. [Citat: den 18 02 2014.] <http://ideas.repec.org/p/wpa/wuwpio/0306001.html>.
35. **Jacobsen, Dag Ingvar.** *Vad, hur och varför*. u.o. : Studentlitteratur AB, Lund, 2002. 9789144040967.

7 Sökord

Avslöjanden, 4

Edward Snowden, 7, 9

FRA, 4, 5, 8, 9

IT-säkerhetspolicy, 15, 17

Massövervakning, 7, 9, 14

NSA, 7, 8, 9

PRISM, 7, 9, 15, 18, 20

Respondent, 14, 15, 16

Studie, 5, 12, 21, 22

UKUSA, 7

Xkeyscore, 9

Öppen källkod, 9, 10, 11, 14, 16, 18, 20

8 Bilagor

8.1 Intervjuguide

Inledande frågor

- Kan ni beskriva er affärsidé och vad ni erbjuder era kunder?
- Vilka är era kunder? Vilka branscher? Storlek etc.?

Ämnesfrågor

- Vad är er uppfattning om övervakningsskandalerna? Har ni påverkats av dem?
På vilket sätt?
- Vad är er generella uppfattning om öppen källkod? Vilka olika uppfattningar finns hos kund?
- Har er uppfattning om öppen källkod förändrats sedan övervakningsskandalerna? På vilket sätt?
- I vilken utsträckning använder ni er av öppen källkod idag?
- I vilken utsträckning erbjuder ni tjänster med öppen källkod?
- Planerar ni att förändra den utsträckningen? På vilket sätt?
- Vilka alternativ till öppen källkod ser ni som kan användas för att garantera säkerheten i era tjänster?
- Kan ni se några andra aspekter som skulle kunna medföra att intresset för öppen källkod förändras?
- Uppskatta hur stor del av kunderna där ni har en tjänst baserad på öppen källkod, helt eller delvis
- Inom vilka typer av era tjänster är öppen källkod mest representerat?
- Anser ni att det finns en koppling mellan öppen källkod och övervakningsskandalerna?