Hendelseshåndtering i små og mellomstore bedrifter

Lars Arne Sand, Gaute Bjørklund Wangen og Anders Sand Frogner

IMT3912 Bacheloroppgave IMT
Bachelor i informasjonssikkerhet
Avdeling for informatikk og medieteknikk
Høgskolen i Gjøvik, 2010

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Sammendrag

Tittel:	Hendelseshåndtering i små og mellomstore bedrifter.	Nr. :
		Dato : 20.05.2010
Deltaker(e):	Lars Arne Sand	
	Gaute Bjørklund Wangen	
	Anders Sand Frogner	
Veileder(e):	Nils Kalstad Svendsen	
Oppdragsgiver:	Norsk Senter for Informasjonssikring	
Kontaktperson:	Tore Larsen Orderløkken	
Stikkord (4 stk)	Hendelseshåndtering, Små og mellomstore bedrifter, Veiledning, Statistikk.	
Antall sider: 185	Antall bilag: 17	Tilgjengelighet (åpen/konfidensiell): Åpen.

Kort beskrivelse av bacheloroppgaven:

Prosjektet er gjennomført på oppdrag fra Norsk Senter for Informasjonssikring. Oppgaven omhandler hendelseshåndtering i små og mellomstore bedrifter. Den undersøker hvordan norske små og mellomstore bedrifter arbeider med hendelseshåndtering, i tillegg gir den en veiledning for hendelseshåndtering rettet mot denne målgruppen.

Undersøkelsen baserer seg på fem forskningsspørsmål. For å besvare disse ble det satt opp fem hypoteser. Konklusjonene for disse hypotesene ble basert på en stor spørreundersøkelse og omfattende dybdeintervjuer. Veiledningen er utarbeidet etter spørreundersøkelsen og dybdeintervjuene, og skreddersydd for målgruppen og dens behov.

Oppgaven førte til følgende konklusjoner:

- Om lag halvparten av virksomhetene har hendelseshåndteringspolicy.
- De fleste virksomheter har dårlig opplæring på hendelseshåndtering.
- De fleste virksomheter har mangelfull eller ingen implementasjon av hendelseshåndtering.
- De fleste virksomheter har dårlige rapporteringsmekanismer, noe som fører til dårlig oversikt over antall sikkerhetshendelser.
- De fleste virksomheter har oppfølging av sikkerhetshendelser.

Konklusjonen på oppgaven ble at situasjonen i norske små og mellomstore bedrifter ikke er så ille som først antatt, men at det fortsatt foreligger mangler og det finnes plass til store forbedringer.

Utvidet sammendrag

Hendelseshåndtering er et spennende og viktig tema innenfor informasjonssikkerhet. Det finnes en del faglitteratur om emnet, men kunnskapen om hvordan hendelseshåndtering anvendes er ikke godt kartlagt. Det var derfor interessant å undersøke dette temaet.

Oppgaven baserer seg på fem forskningsspørsmål. Formålet med disse var å gi innsikt i hvordan små og mellomstore bedrifter anvender hendelseshåndtering. Forskningsspørsmålene fokuserer på om virksomhetene har hendelseshåndteringspolicy, om de har implementering og opplæring innen hendelseshåndtering og om det finnes rutiner for registrering og oppfølging av sikkerhetshendelser. I tillegg til dette gir den en veiledning for hendelseshåndtering rettet mot små og mellomstore bedrifter.

For å besvare forskningsspørsmålene ble det satt opp fem hypoteser. Konklusjonene for disse hypotesene ble basert på resultatene av en spørreundersøkelse og femten dybdeintervju. Veiledningen har blitt utarbeidet etter spørreundersøkelsen og dybdeintervjuene, og er skreddersydd til små og mellomstore bedrifter ut i fra deres ønsker om utseende, format og innhold.

Basert på resultatene av undersøkelsene kom prosjektgruppen frem til konklusjoner på alle fem hypotesene. Om lag halvparten av virksomhetene hadde hendelseshåndteringspolicy, av disse hadde 4 av 5 policyer tilfredsstillende kvalitet. Virksomhetene hadde dårlig opplæring på hendelseshåndtering. Selv om resultatene viste at ca 90% hadde en form for opplæring, var det kun 40% av virksomhetene som hadde opplæring av tilstrekkelig kvalitet. Når det gjaldt implementasjon av hendelseshåndtering, hadde de fleste mangelfull eller ingen implementasjon. Resultatene fra undersøkelsene viste at 60% hadde for dårlige planer, eller ingen planer i det hele tatt. Undersøkelsene viste også at virksomhetene hadde dårlige rapporteringsmekanismer, noe som kan føre til dårlig oversikt over antall sikkerhetshendelser. Til tross for dette, viste undersøkelsen at virksomhetene hadde god oppfølging av sikkerhetshendelser, men resultatene på hypotesen om rapportering ga mistanker om at underrapportering kan ha vært en innvirkende faktor på det positive resultatet i denne konklusjonen.

Konklusjonen på oppgaven ble at situasjonen i norske små og mellomstore bedrifter ikke er så ille som først antatt, men at det fortsatt foreligger mangler og det finnes stort rom for forbedringer. Det kom klart frem fra resultatene at offentlig sektor er de flinkeste når det kommer til hendelseshåndtering. Det viste seg også å være klare fordeler ved å ha en sjef for informasjonssikkerhet. Bedrifter som har dette følger oftere hendelseshåndteringsplanene sine under sikkerhetshendelser, og har generelt høyere kvalitet på planene sine.

Extended abstract

Contingency planning is an exciting and important subject within information security. Although there is some literature about the subject, there is not a lot of knowledge about how small and medium sized enterprises utilize it. Thus the main motivation of this thesis was to uncover how they implemented it, and how well.

The thesis was based upon five research questions. The purpose of these was to examine how small and medium sized enterprises' utilized contingency planning. The subjects covered the enterprises use of contingency planning policy, how well they implemented and educated about contingency planning and how well they registered or followed up security incidents. In addition, the thesis includes a tutorial for contingency planning for small and medium sized enterprises.

In order to answer the research questions, five hypotheses were created. The conclusions for these hypotheses were based upon a questionnaire and fifteen interviews. The tutorial was based upon the questionnaire and interviews, and customized especially for small and medium sized enterprises, out of their desires and requests from the surveys.

The results from the surveys was used to conclude on all five hypotheses. About half of the enterprises had a contingency planning policy, of these, only four out of five had a policy with satisfying quality and content. The enterprises did not have sufficient education within contingency planning. Although 90% had some sort of education, only 40% had education that was sufficient. Concerning the implementation of contingency planning, most of the enterprises had insufficient or no implementation at all. The results of the surveys proved that 60% had insufficient or no plans at all. They also proved that most enterprises had bad reporting mechanisms, something that would lead to a poor overview of the amount of security incidents. Despite this, the surveys showed that the enterprises were good to follow up security incidents.

The conclusion of this thesis was that the situation of Norwegian small and medium sized enterprises is not as bad as first assumed, even though there is big room for improvements. The surveys showed that big enterprises were better in many aspects, as well as the public sector. It also proved that there are advantages of having a chief of information security.

Forord

Oppgaven Hendelseshåndtering i små og mellomstore bedrifter var en oppgave som ble gitt av Norsk Senter for Informasjonssikring til bachelorstudenter på Høgskolen i Gjøvik høsten 2009. Som informasjonssikkerhetsstudenter ønsket prosjektgruppen en oppgave som omhandlet noe innenfor dette temaet, derfor ble oppgaven som NorSIS presenterte valgt.

Prosjektoppgaven har bydd på mange nye utfordringer for alle gruppemedlemmene. Blant annet ble det utført en spørreundersøkelse, dybdeintervju med flere bedrifter, og statistisk analyse av resultatene. Oppgaven bunnet også ut i en veiledning i hendelseshåndtering som er utarbeidet for målgruppen små og mellomstore bedrifter.

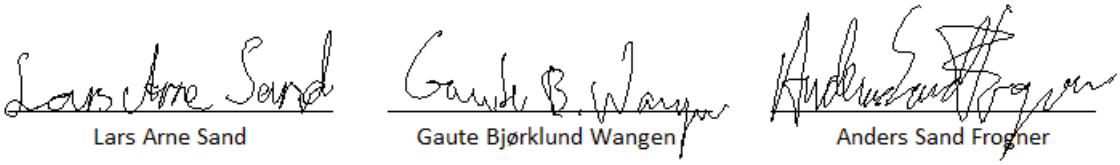
Oppgaven har vært en svært tidkrevende, men også lærerik prosess for alle medlemmene av prosjektgruppen.

Vi ønsker å rette en takk til Nils Kalstad Svendsen, førsteamanuensis ved Høgskolen i Gjøvik, for hjelp og veiledning gjennom arbeidet med prosjektet.

Takk til oppdragsgiver Tore Larsen Orderløkken, leder ved Norsk Senter for Informasjonssikring, for hjelp og støtte gjennom prosjektarbeidet.

Vi ønsker å rette en spesiell takk til alle virksomhetene som tok seg tid til å svare på undersøkelsene våre, uten dere hadde vi ikke klart å gjennomføre dette prosjektet.

Vi ønsker ellers å takke alle andre som har bidratt til prosjektet.



Lars Arne Sand | Gaute Bjørklund Wangen | Anders Sand Frogner

Innhold

Forkortelser og ordforklaringer

Forkortelser:

- SMB - Små og mellomstore bedrifter. Små (0-20 ansatte), mellomstore (20-100 ansatte) [1].
- HMS - Helse, miljø og sikkerhet
- ROS - Risiko- og sårbarhetsanalyse
- IDS - Intrusion detection system (Inntrenger detekterings system)
- BIA - Business Impact Analysis (verdi- og trusselvurdering)
- HiG - Høgskolen i Gjøvik
- NorSIS - Norsk Senter for Informasjonssikring
- CISO - Chief Information Security Officer (Informasjonsikkerhets sjef)
- SIRT - Security Incident Response Team (Sikkerhets hendelseshåndterings gruppe/lag)
- ROSI - Return On Security Investment (Returnering av sikkerhetsinvestering)

Ordforklaringer:

- Sikkerhet - Behold, betryggelse, sikring, trygghet [2].
- Hendelse - Det at noe hender. 2. Tilfeldighet [2].
- Håndtering - Det å håndtere; behandling [2].
- Sikkerhetstiltak - Sikkerhetsforanstaltning [2].
- Kompromittere - Blottstille [2].
- Katastrofe - Ulykkelig vending, fryktelig ulykke [2].
- Veiledning - Dokumentet utviklet av prosjektgruppen 'Veiledning i hendelseshåndtering, håndtering av sikkerhetshendelser for små og mellomstore virksomheter' A.
- ANOVA-analyse - Analysis of Variance [3]. En statistisk analyse hvor en ser på varians mellom grupper.
- Korrelasjonsanalyse - En statistisk analyse hvor en ser på lineære sammenhenger mellom variablene [3].

Definisjoner

Sikkerhetshendelse: hendelse er definert av NorSIS [4] som *Innen informasjonssikkerhet er en 'hendelse' en situasjon som gir, eller som har potensial til å gi, brudd på forventet nivå av konfidensialitet, integritet og/eller tilgjengelighet*. Men i rapporten blir denne definisjonen brukt som *sikkerhetshendelse* for å unngå misforståelser.

Oppdragsgiver: I denne oppgaven refereres det til oppdragsgiver, dette er Norsk Senter for Informasjonssikring(NorSIS [4]).

Veileder: I denne oppgaven refereres det til veileder, dette er oppgavens veileder, Nils Kalstad Svendsen, førsteamanuensis ved Høgskolen i Gjøvik.

1 Introduksjon

Dette kapittelet inneholder informasjon om prosjektoppgaven og hvem prosjektet er skrevet for. Det beskriver formålet med oppgaven, hvilke resultatmål og effektmål som ble satt, samt avgrensninger, rammer og annen informasjon om prosjektet. I tillegg beskrives organiseringen av rapporten og hvordan prosjektgruppen har arbeidet.

1.1 Innledning

De fleste SMBer er mer eller mindre avhengige av IT-systemer. I dagens samfunn lagres mesteparten av kundedata digitalt, enten lokalt eller på nett. Dersom informasjon eller kundedata skulle forsvinne kan det ha store konsekvenser for en virksomhet. Bruken av internett har også økt kraftig de siste årene, [5]. Virksomheter som baserer seg på bruk av internett er avhengige av å ha et oppegående og pålitelig system. Flere typer virksomheter vil også være avhengige av at systemene de innehar opprettholder tilnærmet hundre prosent oppetid. Med slike kritiske faktorer involvert vil det finnes de som vil prøve å utnytte dette. Risikoen for å bli utsatt for forskjellige typer angrep eller sikkerhetshendelser vil være tilstede. Dersom det skulle oppstå en sikkerhetshendelse vil virksomheter være avhengige av å kunne håndtere dette raskt og effektivt, med andre ord, benytte hendelseshåndtering.

Hendelseshåndtering består i hovedsak av fire hovedemner: Verdi og trusselanalyse(Business Impact Analysis(BIA)), Håndtering av sikkerhetshendelser (Incident Response(IR)), Katastrofehåndtering (Disaster Recovery(DR)) og Forsetningskontinuitet (Business Continuity(BC)). Verdi og trusselanalyse består av å identifisere de viktigste ressursene i virksomheten, i tillegg til hvilke trusler som eksisterer og hvordan disse kan påvirke ressursene. I all hovedsak handler denne fasen om situasjonsbevissthet for sine egne ressurser og truslene som eksisterer. Håndtering av sikkerhetshendelser omhandler sikkerhetshendelser av ikke alvorlig grad som kan true virksomheten. Katastrofehåndtering handler om sikkerhetshendelser som kan klassifiseres som katastrofale for virksomheten. Forretningskontinuitet omhandler sikkerhetshendelser av lik alvorlighetsgrad som katastrofehåndtering, men iverksettes bare dersom omplassering/flytting/oppbygging av virksomheten på en alternativ plassering er nødvendig som en følge av sikkerhetshendelsen. Siden sikkerhetshendelser med katastrofale følger er veldig sjeldne, vil vi fokusere på de sikkerhetshendelsene som forekommer mest, og de sikkerhetshendelser virksomheter flest kan takle dersom de har en plan. Dette innebærer sikkerhetshendelser av lav til middels alvorlighetsgrad, altså håndtering av sikkerhetshendelser.

Dette prosjektet vil ta for seg og undersøke hvordan norske SMBer anvender hendelseshåndtering.

1.2 Problemstilling

Etter flere års arbeid med SMBer har oppdragsgiver fått erfare at hendelseshåndtering sjelden er en prioritet. De mener få virksomheter har utarbeidet hendelseshåndteringsplaner, og de som har, sliter med å implementere planene i praksis. Det er på bakgrunn av disse erfaringene at oppgaven er utviklet, og følgende forskningsspørsmål er opprettet:

1. I hvilken grad har virksomheter en hendelseshåndteringspolicy, eller hendelseshåndteringspolicy de følger?
2. I hvilken grad har virksomheter opplæring på hendelseshåndtering?
3. I hvilken grad implementerer virksomheter hendelseshåndteringsplaner?
4. I hvilken grad har virksomheter rapporteringsmekanismer?
5. I hvilken grad har virksomheter oppfølging av sikkerhetshendelser?

For å besvare disse spørsmålene ble det utført en spørreundersøkelse og dybdeintervjuer. Metodikken brukt ved utførelse av arbeidet er beskrevet nærmere under Metodikk2.

1.3 Målgruppe

Denne prosjektrapporten er ment for veileder, oppdragsgiver og generelt alle som har interesse i emnene hendelseshåndtering og informasjonssikkerhet. Veiledningen i hendelseshåndtering retter seg inn mot alle typer SMBer. Veiledningen er ment å være like anvendelig for en IT-bedrift som for en dagligvarebutikk. Ettersom SMBer (*små og mellomstore bedrifter er 0-100 ansatte* [1]) utgjør 99,5% av virksomhetene i Norge [6], er målgruppen relativt stor.

1.4 Formål

Med prosjektrapporten ønsket vi å belyse tilstanden rundt hendelseshåndteringsarbeid i norske SMBer. Dette ville vi oppnå ved å blant annet besvare forskningsspørsmålene. Formålet med veiledningen var å øke bevisstheten rundt hendelseshåndtering i norske SMBer. Det var også ønskelig å opprette en automatisert løsning for innhenting og behandling av undersøkelses data, på denne måten ville oppdragsgiver ha mulighet til å gjennomføre samme undersøkelser ved senere anledninger.

1.5 Effektmål

En virksomhet med gode hendelseshåndteringsrutiner har økt forståelse for egne verdier og truslene den står ovenfor. I tillegg vil de ha bedre evner for å takle eventuelle sikkerhetshendelser som måtte oppstå. Ettersom oppdragsgivers arbeid går på å øke SMBers fokus på informasjonssikkerhet, har hovedeffektmålene til prosjektet vært å øke fokus på hendelseshåndtering generelt hos virksomheter, samt hjelpe virksomheter med å oppnå bedre forståelse for, og rutiner rundt hendelseshåndtering. Prosjektet har blitt utført med følgende effektmål:

- Et større fokus rundt hendelseshåndtering hos SMBer.
- En bredere oversikt over hvordan små og mellomstore bedri fter håndterer forskjellige typer sikkerhetshendelser.
- Øke forståelse og interesse rundt temaet hendelseshåndtering og IT sikkerhet innad i SMBer.
- Få flere SMBer til å implementere og bruke hendelseshåndteringsrutiner.

Ved å oppnå disse målene håper vi å øke fokuset på, samt forbedre forståelsen for, behovet rundt god hendelseshåndtering.

1.6 Resultatmål

For å oppnå effektmålene satt i seksjonen ovenfor, samt besvare forskningsspørsmålene for rapporten, var det nødvendig å utrede spesifikke og etterprøvbare resultatmål. Følgende resultatmål ble utformet:

Ut i fra forskningsspørsmålene ønsket prosjektgruppen følgende resultater for rapporten:

- Rapporten skulle omhandle situasjonen i norske små og mellomstore virksomheter med tanke på hendelseshåndtering.
- Rapporten skulle være et resultat av analysen som ble gjort av spørreundersøkelsen og dybdeintervjuene.
- Den skulle inneholde drøftinger av funnene vi har gjort, med vekt på å besvare forskningsspørsmålene som er gitt i problembeskrivelsen.
- Hvis analysen av spørreundersøkelsen avdekket andre relevante sider ved hendelseshåndtering, skulle disse belyses i rapporten vår.

Etter at veiledningen er ferdig utarbeidet, ønsker prosjektgruppen at den skal gi følgende resultater:

- Veiledningen skulle gjøre utviklingen av hendelseshåndteringspolicy og hendelseshåndteringsplaner lettere.
- Veiledningen skulle være utviklet på en slik måte at den var lett å følge for både små og mellomstore virksomheter.
- Den skulle være kortfattig og lett å implementere.
- Veiledningen skulle ha fokus på det som er viktig for små og mellomstore bedrifter innenfor hendelseshåndtering.
- Den skulle øke virksomhetenes forståelse av problematikken innenfor hendelseshåndtering.
- Veiledningen skulle inneholde minimumstiltak innenfor hendelseshåndtering som er nødvendige i forhold til virksomhetens størrelse.
- Den skulle inneholde forslag til minimumskrav for implementering av deteksjonsverktøy og rapporteringsmekanismer.

Hensikten med resultatmålene, i tillegg til å oppnå effektmålene og besvare resultatmålene, var å gi klarhet i prosjektarbeidet og å gi muligheter for å etterprøve målene. Klarhet i prosjektarbeidet fører til en mer ryddig arbeidsprosess, mens etterprøvbare mål gjør det enklere å måle resultatet av prosjektet.

1.7 Avgrensing

Siden oppdragsgiver hovedsakelig arbeider med informasjonssikkerhet mot SMBer, skulle også prosjektet vinkles mot denne gruppen virksomheter. Med "“hendelseshåndtering"” mener vi verdi og trusselanalyse og håndtering av sikkerhetshendelser. Denne avgrensningen vil gi oppgaven større nytteverdi for SMBer. Det er urealistisk å forvente at SMBer har midler til å ha omfattende katastrofehåndtering eller foretningskontinuitetsplaner. For å begrense størrelsen på oppgaven ble det derfor ikke drøftet katastrofehåndtering i verken veiledningen eller rapporten.

Veiledningen ble avgrenset til små og mellomstore virksomheter for å få et bedre og mer målrettet resultat. Tiltakene i veiledningen ble beskrevet som minimumstiltak, for å begrense lengden, og for å gjøre den gjennomførbar.

1.8 Oppgavebeskrivelse

Hendelseshåndtering har eksistert like lenge som sikkerhetshendelser. Ikke bare har teknologien og trusselbildet forandret seg, men det har også blitt utviklet bedre dokumenterte rutiner for hvordan en bør håndtere sikkerhetshendelser, dette i form at standarder [7] [8] og faglitteratur [9]. Prosjektgruppen skal finne ut om implementering av hendelseshåndtering blir nedprioritert blant norske SMBer, og om de som har implementert rutiner og klarer å følge disse. Det er

på bakgrunn av dette at oppgaven og forskningsspørsmålene 1.2 er utformet. For å besvare forskningsspørsmålene ble det satt opp fem hypoteser (nummerert), og underspørsmål (punkter) for å hjelpe til med å svare på disse:

1. Nesten ingen virksomheter følger hendelseshåndteringspolicy, eller som har hendelseshåndteringspolicy som er tilstrekkelig.
   - Har virksomheten en policy som dekker hendelseshåndtering?
   - Dekker policyen hendelseshåndtering, og er den tilstrekkelig? Det vil si, dekker den de nødvendige aspektene for en god policy. Eksempler på dette er: omfang, roller, ansvar og støtte fra ledelsen.
2. De fleste virksomheter har dårlig opplærling på hendelseshåndtering.
   - Har virksomheten opplæring på hendelseshåndtering?
   - Hvis opplæring finnes, hva slags opplæring og hvor ofte?
3. De fleste virksomheter har mangelfull eller ingen implementering av hendelseshåndtering.
   - Har dere hendelseshåndteringsplaner?
   - Blir disse planene brukt under sikkerhetshendelser?
   - Når blir planen tatt i bruk, finnes det en 'trigger'?
   - Er ansvarsroller fordelt?
   - Er hendelseshåndteringsplanen tilstrekkelig. Det vil si, dekker den de nødvendige aspektene for en god hendelseshåndteringsplan. Eksempler på dette er: omfang, roller, ansvar, trigger, underretning, revidering.
   - Finnes det rutiner for å revidere hendelseshåndteringsplaner eller revidering etter sikkerhetshendelser?
4. Generelt dårlige rapporteringsmekanismer, noe som fører til dårlig oversikt over antall sikkerhetshendelser.
   - Finnes det metoder for å registrere sikkerhetshendelser?
   - Samles sikkerhetshendelser i statistikk?
   - Rapporteres sikkerhetshendelser til ledelsen?
5. Dårlig oppfølging av sikkerhetshendelser er en gjenganger i virksomhetene.
   - Dersom det oppdages en sikkerhetshendelse, gjøres det noe med den?
   - Finnes det et klart fordelt ansvar, eller konsekvenser dersom man ikke følger opp?
   - Har virksomheten vurdert hvordan sikkerhetshendelsen påvirker virksomheten?

Til å besvare hypotesene ble det utført en spørreundersøkelse B og dybdeintervjuer D.

1.9 Prosjektgruppens bakgrunn

Gruppens medlemmer har gått bachelor i Informasjonssikkerhet på Høgskolen i Gjøvik. Prosjektets medlemmer har hatt fagene 'Sikkerhetsplanlegging og Hendelseshåndtering' og 'Risikostyring' som har gitt oss kompetanse på området. Alle stiller også med kompetanse innenfor systemutvikling og programmering. Prosjektgruppen har også benyttet kunnskap tilegnet fra fagene: 'Systemadministrasjon'(IDS og skriping), 'Innføring i Informasjonssikkerhet'(Standarder med mer), 'Dataarkitektur' og 'Operativsystemer'(virtuell maskin og skriping), 'Datakommunikasjon' og 'Sikkerhet i datasystemer'(Kunne se behovene for forskjellige tiltak til veiledningen).

Ingen stilte med kompetanse innenfor statistikk. Det måtte derfor brukes en del tid for å lære dette. Det var også første gangen LaTeX ble brukt av prosjektgruppens medlemmer. Ingen av prosjektgruppens medlemmer hadde utført en stor spørreundersøkelse før, og stilte i utgangspunktet uten kompetanse på dette området. Det å skrive en veiledning var også helt nytt for prosjektgruppen.

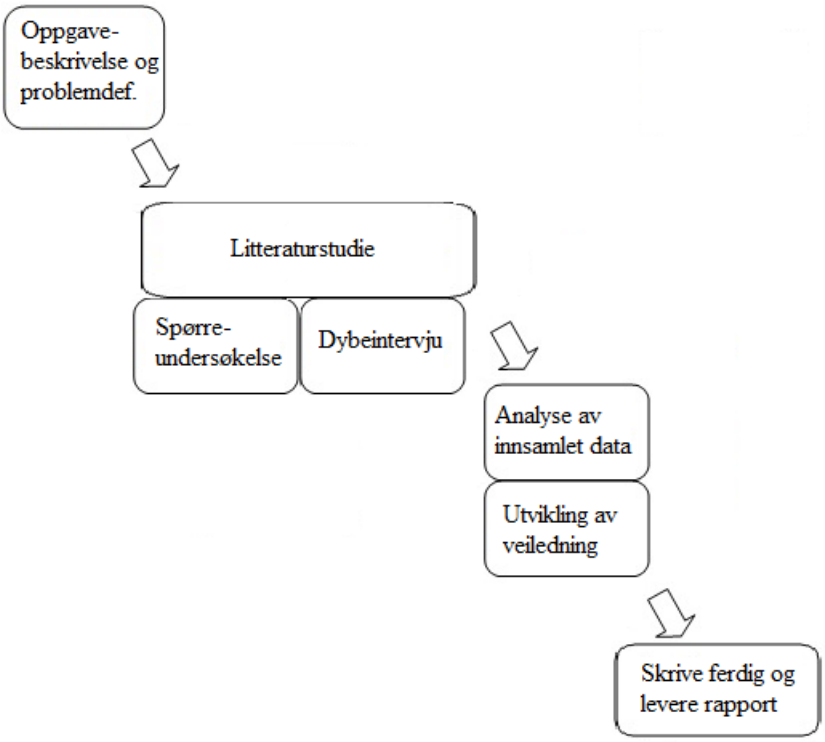
1.10 Rammer

Prosjektet har blitt gjennomført i tidsrommet 5. januar 2010 til 20. mai 2010. Til å utføre spørreundersøkelsen ble Questback [10] brukt, og respondentene i spørreundersøkelsen ble valgt ut i fra kontaktnettverket til oppdragsgiver. Oppdragsgiver stod for innkjøp av standarder og annen litteratur som prosjektgruppa ellers ikke hadde tilgjengelig. LaTeX [11] ble benyttet til å skrive rapporten.

1.11 Arbeidsmetode

Ved valg av arbeidsmetode la gruppen stor vekt på struktur og organisering. Oppgaven var kritisk avhengig av datainnsamlingsprosessen (spørreundersøkelsen og dybdeintervjuene), og at tidsfristene for denne prosessen ble overholdt. Målene som ble satt for oppgaven ville sannsynligvis ikke endres betydelig i løpet av prosjektets gang. På bakgrunn av dette var det derfor ønskelig med en modell hvor vi kunne planlegge alle milepæler og detaljer i en tidlig fase.

Prosjektet har en rapport og en veiledning som sluttprodukt, disse var avhengige av spørreundersøkelsen og dybdeintervjuene. På bakgrunn av dette var behovet stort for klare milepæler. Milepæler vi måtte nå før neste steg kunne utføres. Vi valgte derfor fossefallsmodellen som arbeidsmetode. Modellen passet bra ettersom styrkene til fossefallsmodellen var struktur og organisering, altså de samme egenskapene vi hadde behov for. En stor svakhet i denne modellen var dersom det skulle forekomme endringer. Vi anså ikke dette som noe problem ettersom målene og arbeidet var lett å kartlegge, samt at det var liten sjanse for at dette ville endre seg. Utviklingsmodellen vi fulgte så slik ut 1.



Figur 1: Overordnet utviklingsmodell for hele prosjektet

Planlagt fremdriftsplan vedlegg K, reelle fremdriftsplanen vedlegg L. Utviklingsmodell for veiledningen 6, utviklingsmodell for dybdeintervjuet 5.

1.12 Organisering av rapporten

Prosjektrapporten er strukturert inn i fire kapitler og vedlegg. Struktur og organisering av rapporten har blitt gjort etter en mal for masteroppgaver i informasjonssikkerhet på HiG.

1. **Innledning** Dette kapittelet inneholder grunnleggende informasjon om og presentasjon av prosjektoppgaven.
2. **Metode** Dette kapittelet inneholder metodikken som ble brukt for å løse prosjektoppgaven.
3. **Statistikk** Dette kapittelet inneholder den statistiske analysen og resultatene fra spørreundersøkelsen og dybdeintervjuene, samt drøftinger og konklusjoner av dette.
4. **Avslutning** Dette kapittelet inneholder prosjektgruppas diskusjoner, konklusjoner og oppsummering av oppgaven.

2 Metodikk

Dette kapittelet omhandler metodologien som ble brukt for å besvare forskningsspørsmålene. Dette innebærer utvikling av forskningsspørsmål, oppsett av hypoteser, informasjonsinnsamlingsfase som består av spørreundersøkelse og dybdeintervju, statistisk analyse og hypotesetesting. Videre er metodologien beskrevet for utvikling av veiledning og skripting av statistikk.

2.1 Innledning

Det er vanlig å benytte forskningsspørsmål i artikler eller oppgaver hvor en forsøker å undersøke en påstand eller lære noe nytt om et tema som ikke tidligere er bevist. Ettersom denne oppgaven skal ta for seg hendelseshåndtering, og oppdragsgiver ønsket å lære noe om den nåværende situasjonen i norske SMBer, var det naturlig å bruke en slik tilnærming.

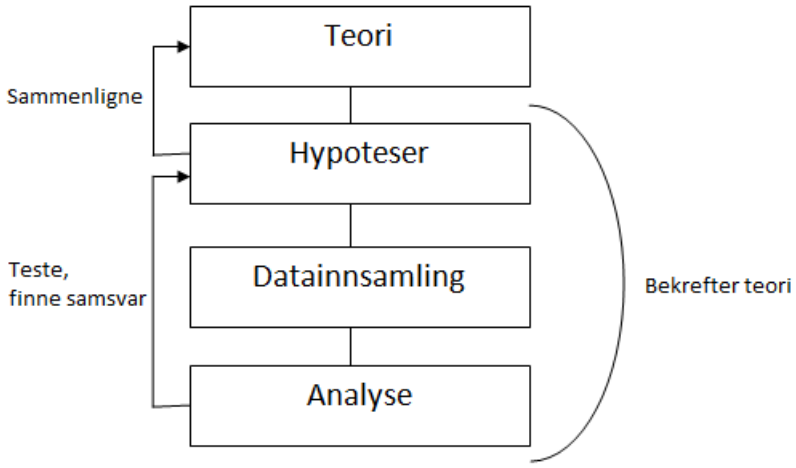
2.1.1 Kartlegging og problemdefinisjon

Forskningsspørsmålene for oppgaven ble utviklet i samarbeid med oppdragsgiver og veileder, på denne måten ble det oppnådd en oppgave som ble så aktuell som mulig for oppdragsgiver, samtidig som prosjektet holder et høyt vitenskaplig nivå. For å besvare forskningsspørsmålene ble det fremsatt hypoteser ut i fra forskningsspørsmålene. Hypotesene beskriver hva som er tilfellet for de forskjellige forskningsspørsmålene. Formålet med undersøkelsen var da å avdekke om hypotesene stemmer med virkeligheten ved å bekrefte/avkrefte hypotesenes sannhet.

Når arbeidet med oppgaven ble igangsatt var det teori rundt hendelseshåndtering og forskningsspørsmålene som dannet grunnlaget for videre undersøkelse og arbeid. Som nevnt, ble det fremsatt hypoteser for å videre undersøke forskningsspørsmålene. For å kunne bekrefte eller avkrefte hypotesene ble det besluttet å foreta en datainnsamlingsprosess. For å gjøre dette ble hypotesene brukt for å utviklet en spørreundersøkelse og dybdeintervju. Fremgangsmåten er illustrert i figur 2.

2.1.2 Informasjonsinnhenting

Spørreundersøkelsen og dybdeintervjuet dannet datainnsamlingsfasen av prosjektet. Med spørreundersøkelsen rettet vi fokuset på å samle kvantitative data. Sammen med dybdeintervjuenes kvalitative datainnsamling dannet disse undersøkelsene en grundig og tilstrekkelig plattform for



Figur 2: Metode for valgt fremgangsmåte. *Oversatt fra [12]*

videre analysearbeid. Spørreundersøkelse og dybdeintervju blir forklart i nærmere detalj i seksjon 2.2 og 2.3

2.1.3 Analyse av informasjon

Statistisk analyse var nødvendig for å klare og trekke konklusjoner på hypotesene, og om hypotesene som ble fremsatt hadde betydelige avvik eller kunne bekreftes. Analyseprosessen besto av en grundig analyse av innsamlede data. Data innhentet fra spørreundersøkelsen og dybdeintervjuene la grunnlaget for analysen. Resultatene av analysen ble testet opp mot de tidligere nedsatte hypotesene. Hypotesene ble på sin side sammenlignet mot forskningsspørsmålene. Ved hjelp av denne metoden kunne prosjektgruppen bekrefte eller avkrefte antagelser og teori. Statistisk analyse blir forklart i nærmere detalj i kapittel 2.5.

2.1.4 Utvikling

Utviklingsfasen besto av 'Veiledning i Hendelseshåndtering' og skript-utvikling til spørreundersøkelsen. Mer om 'Veiledningen i Hendelseshåndtering' finner du i seksjon 2.4. Mer om skriptutviklingen finner du i seksjon 2.6.

2.2 Spørreundersøkelse

Denne delen inneholder metodikken som ble brukt til å utvikle spørreundersøkelsen. Dette innebærer blant annet hensikten bak spørreundersøkelsen, hvordan spørreundersøkelsen ble

utviklet, hvilken målgruppe vi henvendte oss til og struktur/oppbygning.

2.2.1 Hensikt

Spørreundersøkelsen skulle hjelpe oss med å avdekke situasjonen vedrørende hendelseshåndtering i norske SMBer. Hensiktet med spørreundersøkelsen var å hente inn en stor mengde kvantitativ data.

2.2.2 Utviklingsmodell

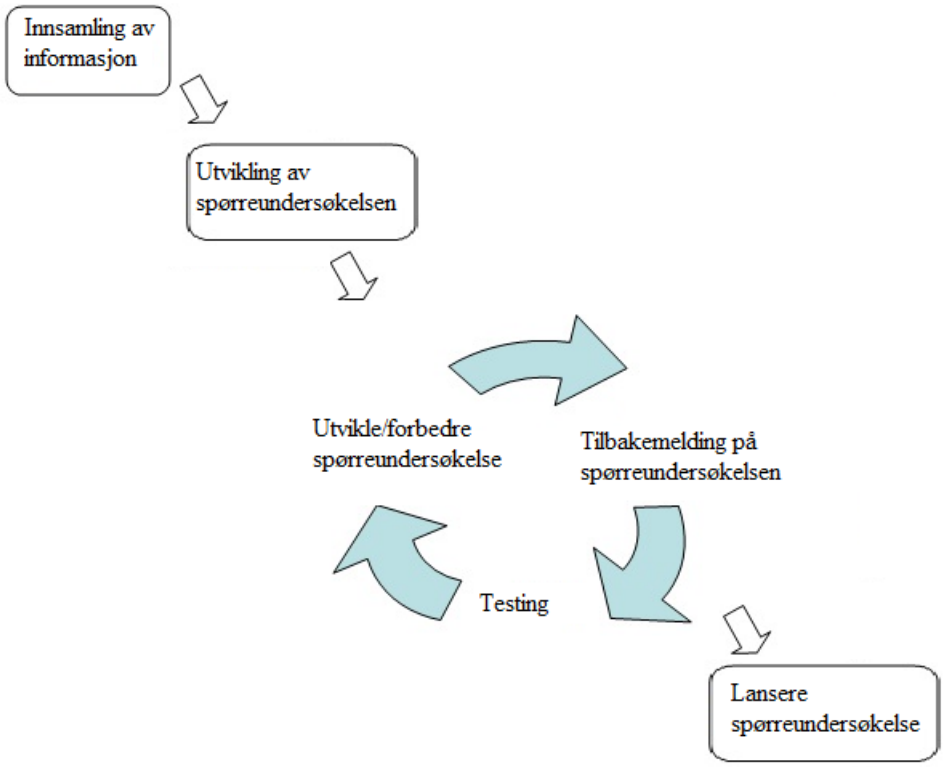
Målet med spørreundersøkelsen var å få svar på så mange forskningsspørsmål som mulig, derfor ble spørsmålene til spørreundersøkelsen laget basert på forskningsspørsmålene. For å utvikle spørreundersøkelsen hadde vi følgende faser:

1. Innsamling av informasjon.
2. Utvikling av spørreundersøkelsen.
3. Utvikling/forbedring, testing og feedback.
4. Lansering av spørreundersøkelsen.

Innsamling av informasjon var en fase som måtte gjøres ferdig før vi kunne fortsette på neste fase som var utvikling av spørreundersøkelsen. Dette var en iterativ fase som hang sammen med testing og feedback, etter spørreundersøkelsen hadde blitt testet og revidert tilstrekkelig, ble den lansert. Modellen er illustrert i figur 3.

2.2.3 Krav

Spørreundersøkelsen kunne ikke være for lang, det kunne gjøre at vi mistet respondenter som kom halvveis ut i undersøkelsen for deretter å gi seg. Respondenten skulle ikke bruke mer enn ti minutter på å fullføre spørreundersøkelsen. Prosjektgruppen bestemte at spørreundersøkelsen skulle utføres online, da dette minsket arbeidsmengden for respondentene, noe i sin tur økte sjansen for at de ville svare på den. Dette forenklet også arbeidet med statistikken i ettertid, da online-spørreundersøkelsen genererer data automatisk, isteden for at prosjektgruppen skulle bruke tid på å skrive inn data fra returnerte spørsmålsark manuelt. Ved å bruke online-undersøkelse fikk vi også svarene umiddelbart. Spørsmålene måtte utvikles på en slik måte at de ble korte og konsise, men fortsatt ga svar på forskningsspørsmålene. Undersøkelsen måtte bestå av spørsmål som hadde enkle alternativer utviklet til statistisk bruk. Questback [10] ble valgt for å utføre spørreundersøkelsen. HiG har en studentavtale med de som gjør at skolens studenter får anvende tjenesten gratis. De har også gode løsninger på fremvisning for spørreundersøkelsen og på respondentanonymitet.



Figur 3: Utviklingsmodell for spørreundersøkelsen.

2.2.4 Målgruppe

Spørreundersøkelsen skulle være rettet mot norske SMBer, men også store norske bedrifter for å få et sammenligningsgrunnlag. For å få flere til å svare på undersøkelsen ble det utviklet og lagt ved et vedlegg i e-posten, se vedlegg C.

2.2.5 Struktur

De innledende spørsmålene ble brukt til å kategorisere bedriftene i antall ansatte og bransje. Resten av spørreundersøkelsen ble strukturert kronologisk etter forskningsspørsmålene og deres underspørsmål, men spørsmålene om hendelseshåndteringsplanene ble lagt til slutt. Spørreundersøkelsen hadde opprinnelig opp mot 45 spørsmål, ifølge kravene i seksjon 2.2.3 besluttet vi at dette var for langt, og svært mange av disse gikk for mye i dybden til å inngå i en online-spørreundersøkelse. Også motivasjonen for å fullføre spørreundersøkelsen ville være større om vi ikke hadde med mange spørsmål. Spørreundersøkelsen ble derfor på totalt 23 spørsmål. Det ble besluttet å ikke ha mer enn 7-8 spørsmål på hver side, slik at det totalt 3 sider. Dette ble gjort for å motivere respondentene til å gjøre ferdig undersøkelsen. Hvert spørsmål ble utviklet med

tanke på statistikk, vi valgte å holde oss til 3 svaralternativer der dette lot seg gjøre. Prosjektgruppa brukte tre svaralternativer, ja og nei. Det ble også lagt til et vet ikke, for å gi respondenten mulighet til å svare dette hvis han/hun ikke visste svaret på spørsmålet [3].

2.2.6 Innhold

De to innledende spørsmålene i spørreundersøkelsen ble brukt til kategorisering av respondentene, i bransje og størrelse. Resten av spørsmålene er basert på forskningsspørsmålene.

- **Policy (spørsmål 3-6):** Disse spørsmålene dreide seg om informasjonssikkerhets- og hendelseshåndteringspolicy, men var kun spørsmål om virksomhetene hadde disse, og om policyen definerte hva en sikkerhetshendelse var. Temaet policy var en del som ble gått grundigere inn på i dybdeintervju, fordi det var lettere å fastslå av hvilken kvalitet policyene har i intervjuform når vi har muligheten til å stille oppfølgingsspørsmål.
- **Opplæring (spørsmål 7-9):** Her startet vi med et flervalgsspørsmål, der vi fikk kartlagt om informasjonssikkerhetspolicy, hendelseshåndteringspolicy og hendelseshåndteringsplaner var inkludert i opplæringen. Dette skulle bli brukt til å få statistikk på hvor mye hendelseshåndtering ble prioritert i opplæringen. Det ble også tatt med et spørsmål om opplæring for ledelsen, siden det er viktig å engasjere ledelsen i hendelseshåndteringsopplæringen. Vi ville også se om dette hadde noe utslag på resultat for bedriftens engasjement i senere spørsmål. Det var også viktig å få statistikk på om virksomheten utførte øvelser basert på planene, siden trening på hendelseshåndtering vil effektivisere selve håndteringsprosessen og få virksomheten tilbake på beina så fort som mulig. Hvilken type opplæring som blir utført og hvor ofte det blir utført opplæring, ble ikke med i spørreundersøkelsen på grunn av at spørreundersøkelsen ikke kunne bli for lang, dette ble tatt med i dybdeintervju.
- **Rapportering (spørsmål 10-15):** Spørsmål 10 var grunnleggende om virksomheten hadde noen rutiner for rapportering. Det ble besluttet å ta med et spørsmål om anonym rapportering, siden det ofte er lettere å rapportere sikkerhetshendelser hvis den som rapporterer forblir anonym, og ikke tar noen form for risiko ved å gjøre det. 12 og 13 angår rutiner for varsling, noe vi fant nødvendig å ha med som et mål på kvalitetene på rutinene. Vi å ta med to spørsmål om hvor mange sikkerhetshendelser som ble registrert og hvor mange som ble rapportert til ledelsen i virksomheten i 2009. Grunnen til at disse to spørsmålene ble med, er at selv om virksomhetene har alle rapporteringsrutiner på plass, er det mulig at ingen bruker de. Svarene på disse to spørsmålene vil da gi oss en indikasjon på om rapporteringen fungerer i praksis eller ikke. Det var også viktig å få kartlagt om ledelsen visste om hvor mange sikkerhetshendelser som rammet bedriften årlig. Det ble besluttet at å spørre om hvilke metoder virksomhetene hadde til å rapportere hendelser egnet seg bedre i dybdeintervju.
- **Hendelseshåndtering (spørsmål 16-22):** Med spørsmål 16 ville vi se om virksomhetene har satt av penger i budsjettet til hendelseshåndtering, med svar på dette spørsmålet ville vi få en indikasjon på hvor mye hendelseshåndteringsarbeid er prioritert i bedriften. Vi brukte

også et spørsmål til å finne ut om virksomhetene har faste personer som håndterer sikkerhetshendelser, som et SIRT eller lignende. Spørsmål 18 ble satt i sammen av tre spørsmål, der vi kategoriserte de under "“etter endt sikkerhetshendelse...'". Her blir det forsøkt å få et innblikk i hvor stor andel av virksomhetene som følger anbefalte retningslinjer etter sikkerhetshendelser. Og om de i det hele tatt har noen form for oppfølging i etterkant av sikkerhetshendelser. Spørsmål 19 blir brukt til å finne ut om virksomhetene har innført noen tekniske løsninger til å detektere sikkerhetshendelser. Resultatet av dette spørsmålet kunne bli interessant å se i sammenheng med antall sikkerhetshendelser de forskjellige virksomhetene hadde. Hvis virksomhetene ikke hadde installert noen form for systemer til å detektere sikkerhetshendelser, kunne de ha sikkerhetshendelser hver dag, uten å selv vite om det. Spørsmål 20 og 21 dreier seg om BIA (Business Impact Analysis), og om virksomheten har utført noe av dette. Det blir spurt om bedriften har utført en risikoanalyse og en verdianalyse. Dette er to hjørnesteiner i sikkerhetsarbeid innenfor bedrifter, og er et minimum innenfor analysering av bedriftens verdier og svakheter. Med spørsmål 22 ville prosjektgruppen finne ut om virksomhetene har beskrevet konsekvenser hvis ansatte bryter sikkerhetsregler. Dette går direkte på oppfølging av sikkerhetshendelser.

- **Virksomhetens evne til å håndtere sikkerhetshendelser (spørsmål 23):** Dette spørsmålet ble brukt for å gi respondentene mulighet til å vurdere sin egen bedrifts evne til å håndtere sikkerhetshendelser. Spørsmålet ville også gi oss et innblikk i hvordan virksomhetene selv mener de håndterer sikkerhetshendelser.

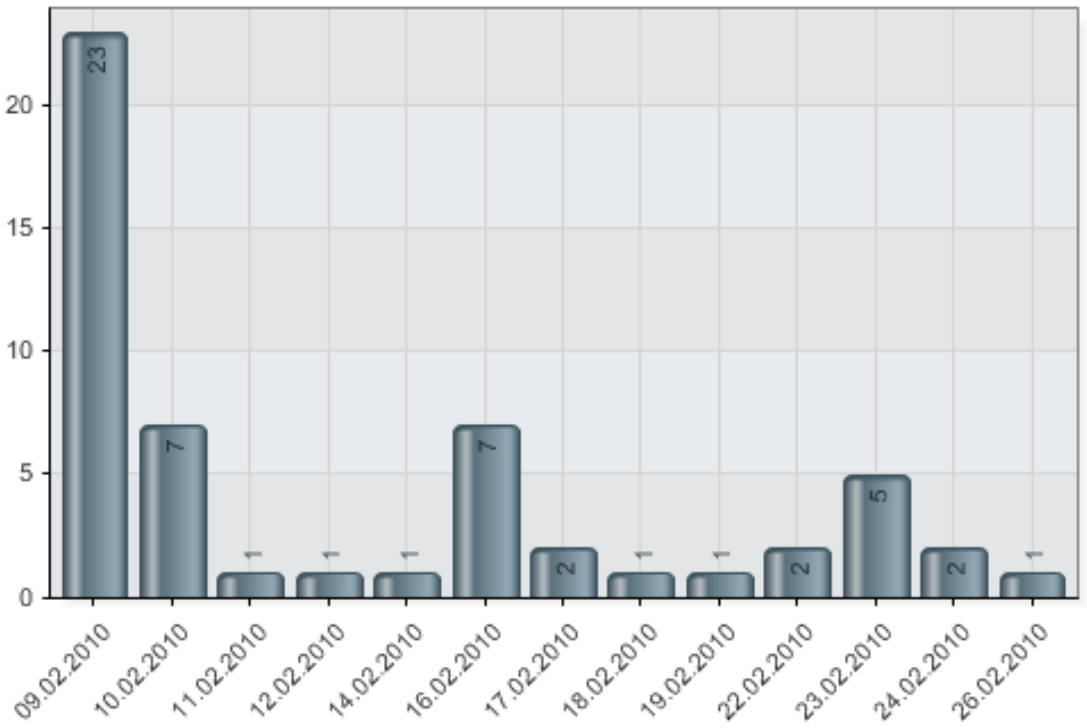
2.2.7 Kvalitetssikring

Før spørreundersøkelsen ble sendt ut, ble den kvalitetssikret. Spørsmålene ble først utviklet av prosjektgruppen, deretter diskutert av veileder og oppdragsgiver. Etter en diskusjon med forslag til forbedring, ble endringer utført. For kvalitetssikring av spørreundersøkelsen er det viktig å kjøre en pilotundersøkelsen [3]. Denne pilotundersøkelsen ble sendt til en testgruppe som svarte på den og ga feedback. Prosjektgruppen testet også utsendingssystemet til Questback før undersøkelsen ble sendt ut til respondentene, for å være sikker på at utsendingen ble riktig.

2.2.8 Valg av respondenter

Når det skulle velges ut respondenter ble kontaktnettverket til NorSIS satt til disposisjon for prosjektgruppa. Vi valgte respondenter fra alle sektorer for å få et resultat som representerte tverrsnittet av norske SMBer. Spørreundersøkelsen ble sendt til 12 store, 69 mellomstore, og 67 små, totalt 148 virksomheter.

Spørreundersøkelsen ble sendt ut den 9.2.2010. Deretter gikk det en uke før første purring(16.2.2010) ble sendt ut. Det ble sendt ut en tredje purring to uker etter at spørreundersøkelsen ble publisert. Spørreundersøkelsen ble avsluttet den 27.2.2010. Oversikten over når respondentene svarte vises i figur 4.



Figur 4: Oversikt over antall respondenter (Y-aksen) per dag (X-aksen).

Som vi ser ut i fra grafen var det høy svarprosent første dagen og andre dagen. Deretter ble det bare en og ingen respondenter dagene før første purring. Når første purring ble sendt ut økte antall responder, og vi ser samme tendensene mot neste purring, og ved siste purring får vi med noen til. Siden prosjektgruppa hadde press på seg til å få avsluttet spørreundersøkelsen, ser vi i ettertid at vi fikk dårlig respons dagene i etterkant av e-post utsendelsene. Vi kunne sendt ut purringene med bare 4 dagers mellomrom, hadde vi gjort det kunne vi avsluttet undersøkelsen i løpet av 2 uker. Som konsekvens av dette kunne prosjektgruppen fått en uke bedre tid til å jobbe med dybdeintervjuet.

2.3 Dybdeintervju

Denne delen av metode inneholder fremgangsmåte og metodikk for arbeidet med dybdeintervju. Dette innebærer blant annet hensikt, utviklingsmodell, krav, målgruppe og struktur. Dybdeintervjuene ble utført for å få svar på alle hypotesene, inkludert de vi ikke tok for oss under spørreundersøkelsen.

2.3.1 Hensikt

Dybdeintervjuene består av femtitre spørsmål, og er delt opp i fem deler, hver del er skrevet for å besvare de forskjellige hypotesene. Deler av dybdeintervjuet ble også rettet mot veiledningen vi skulle utvikle, inkludert spørsmål som ikke nødvendigvis dekket forskningsspørsmålene eller hypotesene. Allikevel må disse ses på som nødvendige supplementer. Denne typen spørsmål ble brukt for å danne et bedre bilde av hendelseshåndteringen, og ble brukt for å kunne utvikle veiledningen. Hoveddelen av dybdeintervjuet baserer seg på spørsmålene rettet mot underspørsmålene og hypotesene, som igjen er basert på forskningsspørsmålene.

2.3.2 Utviklingsmodell

For å utvikle dybdeintervjuet identifiserte vi fem forskjellige faser:

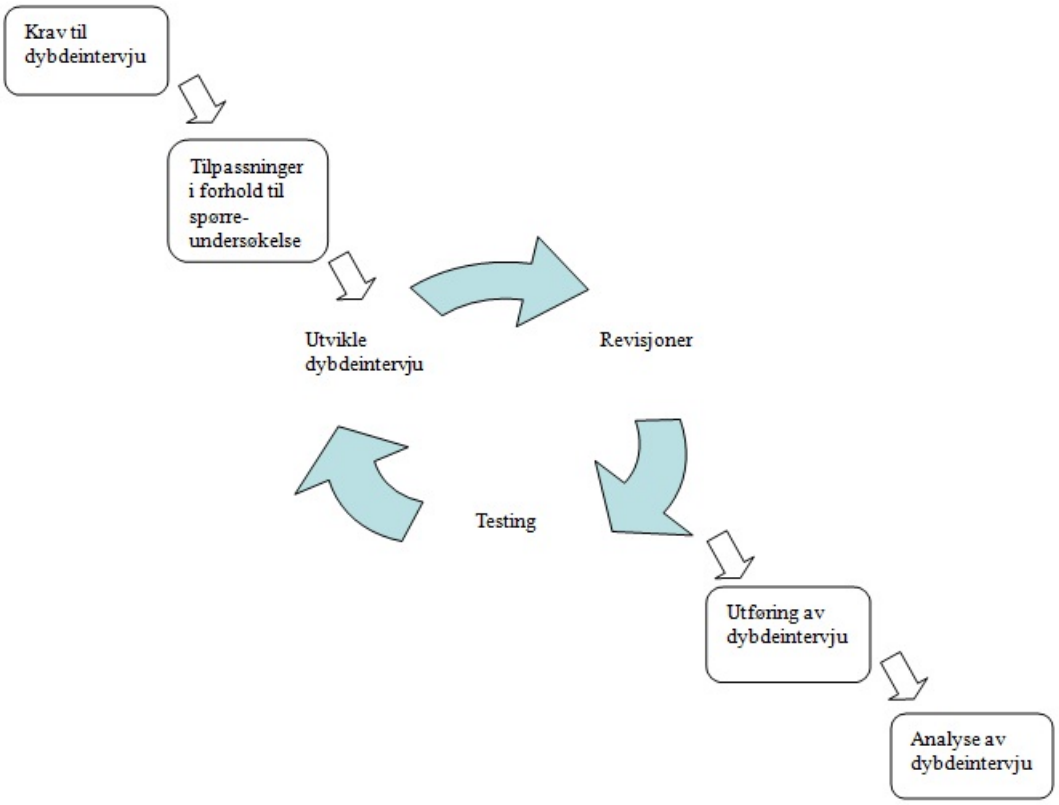
1. Krav til dybdeintervju.
2. Tilpasninger i forhold til spørreundersøkelse.
3. Utvikle dybdeintervju.
4. Utføre dybdeintervju.
5. Analysere resultater.

Krav til dybdeintervju måtte bestemmes først, for at dybdeintervju deretter skulle tilpasses spørreundersøkelsen slik at disse utfylte hverandre til den grad at alle hypotesene ble tilstrekkelig besvart. Deretter ble det planlagt en iterativ fase med utvikling av dybdeintervjuet som innebar testing og revisjoner. Etter prosjektgruppen fastslo at dybdeintervjuet var tilstrekkelig kvalitetssikret, ble det tatt i bruk til å intervjue femten virksomheter. 5

2.3.3 Krav

Kravene til dybdeintervju går i stor grad ut på hvilke krav vi hadde til utformingen og utførelsen av intervjuene. Et av de viktigste kravene var at intervjuene skulle utføres på en nøytral måte. Utførelsen av intervjuene skulle på ingen måte påvirke intervjuobjektene, og som konversasjonsfører skulle vi ikke på noen måte bli påvirket av respondenten. Dette ville vært uheldig ettersom det til en viss grad kunne påvirket datainnsamlingsprosessen, og med dette gjøre analysen feilaktig.

Det ble lagt stor vekt på utforming av spørsmålene til dybdeintervjuet, og hvordan de ble presentert. Spørsmålene som ble utformet skulle til en så stor grad som mulig være vitenskapelige, samtidig som de kunne appellere til intervjuobjektene. Det ble lagt vekt på at de fleste som deltok på dybdeintervjufasen ikke var IT virksomheter, og spørsmålene måtte være deretter.



Figur 5: Utviklingsmodell for dybdeintervju

2.3.4 Målgruppe

Vi var ute etter et bredt spekter av forskjellige typer virksomheter innenfor forskjellige type sektorer. Det å begrense seg innenfor få sektorer vil potensielt påvirke informasjonen vi samlet inn og skape et feil bilde. Størrelsen på virksomhetene ble også naturlig nok vektlagt, siden oppgaven omhandler norske små og mellomstore virksomheter. Fokuset vårt ble rettet mot virksomheter som lå på under hundre ansatte [6]. Vi intervjuet femten forskjellige virksomheter, fordelt over et tverrsnitt av forskjellige bransjer. To av virksomhetene var store, de tretten andre virksomhetene var små og mellomstore virksomheter. Vi ville blant annet undersøke om det fantes stor forskjell vedrørende hendelseshåndtering mellom de store virksomhetene og SMBer, og dersom det gjorde det, måle de store opp mot SMBer. Dybdeintervjufasen er en fortsettelse på spørreundersøkelsen, og sikter inn på å avdekke informasjon vi ikke fikk svar på under spørreundersøkelsen. Under spørreundersøkelsen var det tydelig at IT virksomheter og offentlige virksomheter generelt stilte sterkt innenfor hendelseshåndtering, spesielt i forhold til andre typer virksomheter. Som følge av dette valgte vi som nevnt tidligere å intervjue et bredere spekter og inkludere flere forskjellige type bransjer.

Vi startet utvelgelsesprosessen ved å bruke samme kontaktliste som ved spørreundersøkelsen. Denne listen med virksomheter var et bidrag fra oppdragsgiver, for å gjøre det enklere for prosjektgruppen å plukke ut aktuelle virksomheter. Listen inneholdt en stor del IT virksomheter. Vi kontaktet de virksomhetene som lå inn under andre type bransjer. De vi kontaktet angående deltagelse viste liten vilje til å delta på en litt større undersøkelsesfase. Siden viktigheten av å intervjue virksomheter innenfor andre bransjer enn IT var stor, så vi oss nødt til å utvide utvelgelsen vår. Det ble tatt kontakt med flere virksomheter i nærmiljøet og virksomheter vi hadde et tidligere kjennskap til. Intervjuene ble utført med disse virksomhetene.

2.3.5 Struktur

Dybdeintervjuet er strukturert ut fra forskningsspørsmålene. Dybdeintervjuet åpner med noen generelle spørsmål rundt virksomheten, deretter med spørsmål rettet mot hypotesene. Alle spørsmålene er utviklet slik at man skal kunne besvare spørsmålet utdypende, det vil si, unngå 'ja' , 'nei' og 'vet ikke' type svar. Dybdeintervjuet avslutter med fem spørsmål angående veiledning om hendelseshåndtering og hvordan respondenten tror virksomheten takler en sikkerhetshendelse.

2.3.6 Argumentasjon

Det største argumentet bak valget av dybdeintervjuformen er at vi fikk muligheten til å stille kontrollspørsmål. Kontrollspørsmålene ble brukt for undersøke om de forskjellige virksomhetenes definisjoner stemte overens med prosjektgruppens oppfattning av hendelseshåndtering. Kontrolspørsmålene ble også brukt for å finne ut av omfanget av planene og rutinene til virksomhetene. Det ble tidlig oppdaget at forskjellige virksomheter har forskjellige oppfatninger og definisjoner rundt temaene vi undersøker, det var derfor meget viktig at vi fikk konstatert hvilke definisjoner de forskjellige virksomhetene brukte. Med dybdeintervju hadde vi også muligheten til å gå dypere inn på hendelseshåndtering og diskusjoner rundt tema enn vi ville hatt om vi kun hadde hatt fokus på spørreundersøkelse.

2.3.7 Innhold

Innholdet i dybdeintervjuet ble i stor grad påvirket av spørreundersøkelsen. For å få et grundig svar på alle hypotesene vi hadde satt oss var det nødvendig å spørre en del spørsmål, og forhøre oss om en del temaer som ikke nødvendigvis passet godt under spørreundersøkelsesformen. De temaene og punktene som manglet fra spørreundersøkelsen ble dermed hovedfokus under dybdeintervjuet:

- Kvaliteten på hendelseshåndteringspolicy
- Dybdespørsmål rundt opplæring

- Kvalitet på hendelseshåndteringsplaner
- Revisjon av planer
- Rapporteringsmekanismer
- Virksomhetens tiltak under og i etterkant av en sikkerhetshendelse
- Debriefing
- Backup planer og rutiner

2.3.8 Kvalitetssikring

Bachelorgruppen gjennomførte et møte med Professor II Berhard Hämmerli og veileder angående utformingen av dybdeintervjuet, og hvordan vi skulle gå frem når vi utførte selve intervjuene. På møtet ble det drøftet viktige aspekter vi burde fokusere på, og hvordan målene for dybdeintervjufasen skulle oppnås. I løpet av dybdeintervjuets utviklingsfase har vi hatt flere dype gjennomganger av de forskjellige spørsmålene, og kontrollspørsmålene vi ville bruke. Dybdeintervjuet gikk gjennom mange revisjoner, og det ble arbeidet grundig med utformingen av spørsmålene og struktur. Det ble utført en testrunde hvor en annen bachelor gruppe på HiG besvarte spørsmålene i dybdeintervjuet, på denne måten fikk vi et tidsestimat, og en tilbakemelding på flyten i intervjuet. Når det kom til selve utformingen av spørsmålene, og hvordan de skulle stilles, la vi mye fokus på at vi skulle holde oss så nøytrale som mulig. Vi ville oppnå at intervjuobjektene pratet fritt rundt spørsmålene. Vår hovedoppgave under intervjuene var å sørge for å styre samtalen, og sørge for at intervjuobjektene svarte på temaene vi undersøkte.

2.3.9 Fremgangsmåte

Intervjuene ble utført over telefon eller ved oppmøte hos virksomhetene. Intervjuene varte i alt fra tjue til førtifem minutter. Intervjuene ble utført på en slik måte at intervjuobjektet skulle kunne snakke fritt rundt spørsmålene. Målet vårt var å fungere mer som en konversasjonsstyrer enn en intervjuer. Med dette ønsket vi at intervjuobjektene skulle kunne komme med egne meninger om hendelseshåndtering, og få bedre flyt i intervjusamtalen. Ved bruk av denne metoden var målet å lettere kunne få frem oppriktige meninger, arbeidsmetoder, planer og rutiner til de forskjellige virksomhetene. Både under telefonintervju og ved oppmøte var det alltid to gruppemedlemmer fra bachelorgruppen tilstede, hvor én førte intervjuet, tok den andre notater. Valget om å ikke bruke båndopptager var bevisst, og ble gjort med tanke på norske lover og regler som eksisterer rundt avlytting, samt at det ville være lettere å komme i samtale med intervjuobjektene dersom de ikke følte de ble presset til å ordlegge seg formelt. Før intervjuene ble igangsatt ble det opplyst at all data ville bli behandlet konfidensielt, og at virksomheten og respondenten ville bli tilsendt intervjuet med svarene for etterkontroll. Dette skulle også være med på å få respondenten til å føle seg trygg på hva man kunne fortelle, som igjen vil sørge for

at resultatet av datainnsamlingen i større grad blir korrekt.

2.3.10 Analyse

Når prosjektgruppen utarbeidet problemstilling, forskningsspørsmål og hypoteser satt vi også opp underspørsmål til hypotesene. Svar på disse underspørsmålene ville kunne gi et tydelig svar på hypotesene vi hadde utviklet. Tanken bak dette var at vi ved analyse av dybdeintervjuet skulle kunne bruke svarene vi fikk fra dybdeintervjuene til å besvare underspørsmålene, disse underspørsmålene skulle gi oss svar på hypotesene.

Vi valgte denne formen for oppsett for å lettere kunne analysere svarene. Med analysen av dybdeintervjuene, sammen med spørreundersøkelsen kunne vi i stor grad besvare underspørsmålene vi satte opp, og med det, også svare på hypotesene. Med mengden dybdeintervjuer vi utførte fikk vi nok data til å være i stand til og trekke konklusjoner.

Det ble antatt at de to store virksomhetene vi intervjuet ville ha et bedre utgangspunkt for å ha god hendelseshåndtering. På denne måten ville vi kunne sammenligne de små og mellomstore opp mot de to store virksomhetene.

Informasjonen hentet ut fra dybdeintervjuene ble brukt for å kunne utvikle en fullstendig veiledning, og også som bakgrunnsinformasjon for å kunne nå en konklusjon i rapporten.

2.4 Veiledning

I denne seksjonen er det informasjon om hvordan veiledningen A ble utviklet. Seksjonen inneholder fremgangsmåter og metodikk. Dette innebærer blant annet hensikt, utviklingsmodell, krav, målgruppe og utvikling.

2.4.1 Hensikt

Hensikten med veiledningen er å forenkle utvikling og implementering av hendelseshåndteringsplaner for SMBer. Den skal gi virksomhetene et innsyn i minimumskrav som settes til utvikling av hendelseshåndteringsplaner.

2.4.2 Utviklingsmodell

Det ble gjort søk etter en spesifikk utviklingsmodell for å utvikle veiledning, det ble blant annet kontaktet en autoritet på dette området [13], denne autoriteten visste dessverre ikke om noe slikt. Det ble funnet noen artikler som omhandlet emnet på Internett, disse beskrev i detalj

hva en veiledning burde inneholde og inneholdt noen konkrete tips for arbeid og utvikling av veiledningen [14, 15].

Denne oppgaven går ut på å strukturere et dokument som skal brukes av SMBer i Norge. Dokumentform ble bestemt ut i fra svar på dybdeintervju som vi utførte med 15 virksomheter. Vi så for oss tre sekvensielle faser der den ene måtte være ferdig før den andre kunne påbegynnes. Disse tre var:

1. Innsamling av informasjon.
2. Litteraturstudie.
3. Bestemme innhold og struktur.

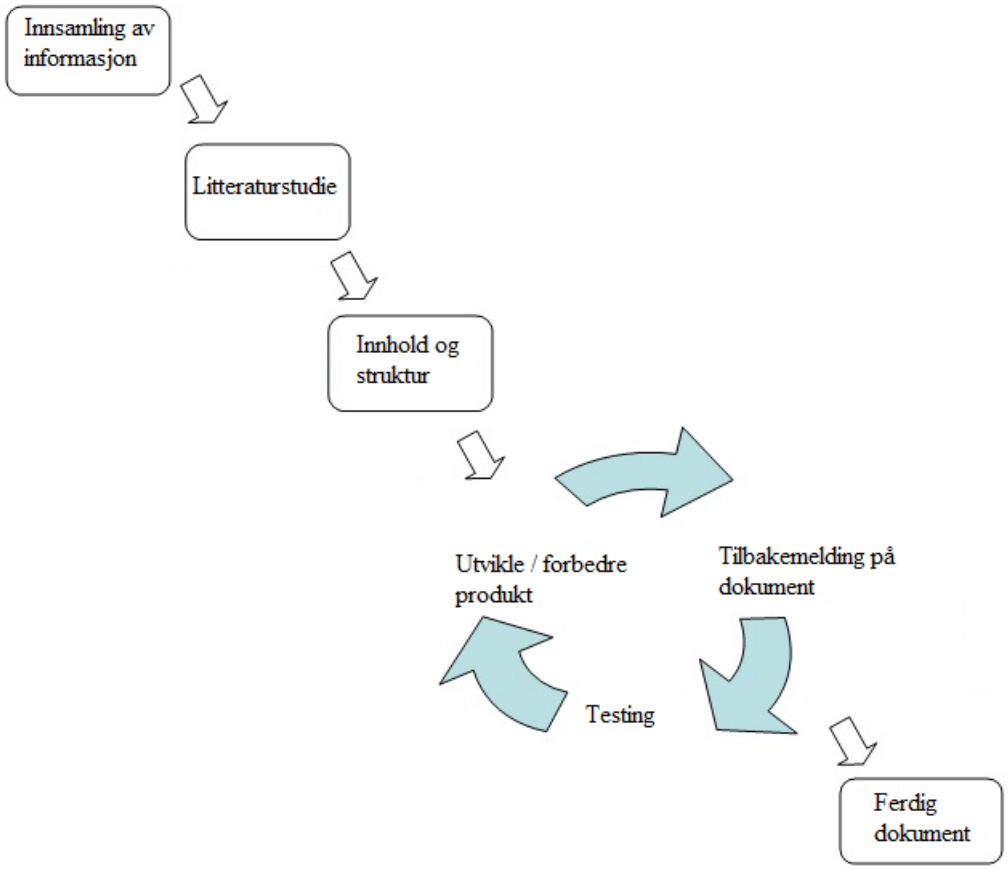
Derfor var det ønskelig med en sekvensiell modell for disse tre første stegene. Gruppen består bare av tre personer, derfor var ikke de utviklingsmodellene som er basert på store utviklingsgrupper aktuelle. Gjenbruksmodellen er mer tiltenkt kodingsprosjekt, men ble delvis benyttet ettersom vi brukte en del teori og struktur fra Whitman og Mattords bok [9] og NIST 800-34 [8]. Vi skulle heller ikke dele opp dokumentet i inkrementer under utviklingen, så den inkrementelle modellen var heller ikke aktuell. Valget av modell falt da på fossefallsmodellen for de tre første stegene i utviklingen av veiledningen.

Etter disse tre kom det en iterativ fase, hvor vi jobbet i samarbeid med veileder og oppdragsgiver med utviklingen av dokumentet. Denne fasen gikk ut på at vi hadde ukentlig innspill på utviklingen av dokumentet, der vi gjorde endringer ut i fra hva veileder og oppdragsgiver ønsket. Vi testet også veiledningen ute i en virksomhet, og fikk tilbakemelding fra dem. Etter tilbakemeldingsfasen var ferdig, sto vi igjen med et ferdig dokument. Vi ble tilslutt stående igjen med en hybrid av fossefallsmodellen og en iterativ modell. Modellen er illustrert i figur 6.

2.4.3 Krav

Hovedfokus for veiledningen var å gi innspill på, og forenkle utvikling og implementeringen av hendelseshåndteringsplaner for SMBer, og få større fokus rundt dette temaet. Det ble satt høye krav til kvaliteten på veiledningen av oppdragsgiver, fordi det ferdige produktet skulle legges ut som en veiledning på oppdragsgivers egne hjemmesider. Arbeidskravet i antall timer ble høyt for å få veiledningen opp til kvalitetskravene. Det ble satt også krav til at veiledningen var enkel i struktur, lett leselig, samt at innholdet var av høy kvalitet.

Et av de viktigste kravene var at veiledningen måtte kunne utnyttes i praksis, og være lett anvendelig for de fleste SMBer. Veiledningen måtte begrenses i lengde, ellers risikerte den å falle i samme kategori som de tunge standardene som allerede er tilgjengelige. Forskjellen mellom standarden [8] og veiledningen A var at standarden inneholder all informasjon som en stor



Figur 6: Fossefallsmodell med en iterativ fase.

bedrift trenger for å implementere solide hendelseshåndteringsplaner. Problemet med dette er at det blir for mye arbeid for SMBer, de kan få trøbbel med å skille ut hva som er viktig og hva som er mindre viktig. Veiledningen inneholder derfor et minimum av informasjon, der kun det nødvendigste er tatt med, og den er rettet mot SMBer.

Innholdet i veiledningen måtte stamme fra forskningsbasert teori, og hvis det ikke gjorde det, måtte vi ha solid argumentasjon for hvorfor vi skulle ha med de øvrige punktene. Oppdragsgiver ville at veiledningen skulle bli en 'miniversjon' av det stoffet som allerede lå ute.

Krav som ble satt av bedriftene vi intervjuet var at den skulle være praktisk anvendelig og enkel. Det ble også nevnt krav til at den ikke var for lang. Noen ville også ha med maler for å se hvordan en policy og en plan kan se ut.

Prioriteringen i designet var at den skulle være lett å lese med punktvis opplisting av krav. Kapitlene måtte komme kronologisk etter hverandre for enklest mulig implementering.

Veiledningen skulle også testes ute hos en bedrift før den kunne publiseres.

2.4.4 Målgruppe

Veiledningen har blitt tilpasset til små og mellomstore bedrifter som i utgangspunktet har svært lite eller ingen form for hendelseshåndtering innført. Formatet på veiledningen ble valgt av virksomhetene selv. Størrelsen vi så for oss på veiledningen var ikke mer enn 10 sider for at det ikke skulle bli et for tungt dokument. Vi tror også at det er større mulighet for at virksomhetene faktisk utfører stegene som er beskrevet i veiledningen hvis den ikke er for lang og tung, slik som vi mener blant annet NIST 800-34 [8] er. Stegene som blir beskrevet i veiledningen er også beregnet på personer som aldri har jobbet med hendelseshåndtering. Veiledningen er hovedsakelig ment for å brukes av ledelsen i SMBer. Veiledningen er rettet mot de som skal utføre hendelseshåndteringsarbeid i bedriften, både ledelse, teknikere og andre. Siden veiledningen skal kunne benyttes i forskjellige ledd i virksomheter, er språket vi har brukt forståelig for de fleste, uansett akademisk bakgrunn eller hvilken arbeidserfaring man har skal man kunne bruke veiledningen. Dette har også blitt gjort for at den skal være anvendelig for tverrsnittet av norske SMBer.

Innholdsmessig har vi lagt vekt på å forklare de forskjellige kapitlene kort og konsist, for å gjøre det lettest mulig å forstå. Stegene som blir beskrevet i veiledningen er også beregnet på personer som aldri har jobbet med hendelseshåndtering før. Vi har unngått å inkludere tunge steg i veiledningen, dette har vi gjort ved å dele opp store kompliserte steg inn i flere små enkle steg.

2.4.5 Utvikling

Navnet som ble satt på veiledningen var *Veiledning i hendelseshåndtering, håndtering av sikkerhetshendelser for små og mellomstore bedrifter*. Navnet beskriver innholdet i, og meningen med dokumentet på en kort og presis måte. Vi gjorde oss opp noen tanker i forkant av utviklingen av veiledningen, hvordan den skulle se ut og hvilket format den skulle ha. For å få hjelp til å velge format på veiledningen ble det lagt til to tilleggsspørsmål på slutten av dybdeintervjuet der det ble spurt om: 'Hvis du skulle utviklet en hendelseshåndteringsplan, hva slags veiledning kunne du tenkt deg?' og 'Hvilket format ville du foretrukket å hatt veiledningen i?'. På det første spørsmålet svarte sju av femten at de ville ha en praktisk og enkel veiledning der det ble beskrevet trinnvis hva som skal gjøres, det ble også lagt vekt på at den skulle være så lite byråkratisk som mulig. Vi tok dette til etterretning siden de åtte andre virksomhetene som deltok på intervjuet hadde svært forskjellige eller ingen meninger om temaet. Det overordnede formatet som ble foretrukket var word- og pdf-dokumenter med illustrasjoner, ble det valgt pdf-formatet siden det gir et fint og ryddig layout.

Det ble diskutert om det skulle lages to separate veiledninger, en for små virksomheter og en for mellomstore. Et argument for å lage to forskjellige veiledninger var at vi får mer spesialiserte

veiledninger. De mellomstore ville fått en litt mer komplisert veiledning enn de små. Men etter mye arbeid med teorien rundt utviklingen av hendelseshåndteringsplan innså vi at veiledningene ville bli svært like. Det var bare noen få punkter som hadde blitt forskjellige, og dette var ikke tilstrekkelig argumentasjon til å utvikle to separate veiledninger. Derfor ble det besluttet å heller gi ut en lik for begge typer virksomheter. Dette var lettere for oss, samt at vi sparte tid uten at det fikk store konsekvenser for resultatet. For å utvikle veiledningen etter ønske fra bedriftene og gjøre den så enkel som mulig, måtte vi se på minimumskravene til en hendelseshåndteringsplan. Overordnede krav satt til veiledningen var at den skulle være så kort og konsis så mulig for å motivere leserne av veiledningen.

2.4.6 Struktur

Ved hjelp av Whitman og Mattords bok [9] og NIST SP 800-34 [8] ble det identifisert 7 overordnede punkt i utviklingsprosessen av en hendelseshåndteringsplan som var essensielle for at den skulle bli tilstrekkelig. Disse ble valgt fordi vi tidligere hadde kjennskap til dem fra faget IMT3521 Sikkerhetsplanlegging og Hendelseshåndtering, og det ligger mye testing og etterprøving av denne teorien i grunn før den ble publisert. Vi kunne heller ikke kutte ut noen av de 7 punktene uten av veiledningen gikk ned i kvalitet. Mye av problemet til NIST 800-34 [8] var at deres underpunkter var for tunge å implementere for SMBer. En stor del av jobben ble å skjære ned på disse og bare beholde det som var essensielt i veiledningen for å utvikle en funksjonabel og tilstrekkelig hendelseshåndteringsplan. Oppdragsgiver ville at vi lagde et eget kapittel i veiledningen der vi kommenterte outsourcing. Dette kapitlet / telet skulle kommentere hvilke krav som settes til databehandlere ved outsourcing og hvilke lover som gjelder. Hensikten med dette kapittelet var å klargjøre hva virksomheter bør ta hensyn til og hva som bør stå i kontrakten før de eventuelt outsourcer noe. Trusselscenario kapittelet ble tatt med etter forespørsel fra oppdragsgiver for å øke bevisstgjøring rundt temaet hendelseshåndtering.

Som nevnt tidligere valgte vi å bare lage en veiledning for både små og mellomstore virksomheter, men vi valgte å skille mellom viktige og mindre viktige steg i de ni kapitlene. Dette gjorde vi ved å utheve de viktigste i tykk skrift. På denne måten fikk vi uthevet de absolutte minimumskravene for hvert steg. De som da har dårlig tid og / eller lite ressurser til å utvikle planer kan da dra nytte av disse viktigste punktene, og de som har bedre tid og mer ressurser kan utføre alle punktene i veiledningen. Veiledningen ble bestående av en innledning med underpunkter, og ni kapitler, disse ni ble:

1. Utvikling av hendelseshåndteringspolicy
2. Verdi og trusselvurdering
3. Forebyggende tiltak
4. Utvikle gjenopprettingsstrategier
5. Utvikle en hendelseshåndteringsplan

6. Øvelser og opplæring
7. Vedlikehold av plan
8. Outsourcing
9. Trusselscenarioer

Det har vært fokus på å være korte og konsise i de forskjellige kapitlene for å holde veiledningen på et minimum når det kommer til størrelse. Dette ble gjort for at det skulle bli lettere og mer motiverende for bedriftene å lese igjennom veiledningen, og for å prøve å unngå tilfeldige misforståelser av teori som kan oppstå hvis teorien er tung å fordøye. Som struktur i hvert kapittel ble det valgt å ha med en innledningen, hvor det blir forklart hvorfor innholdet i dette kapittelet er viktig og bør gjennomføres. Punktvis fremgangsmåte ble valgt der dette lot seg gjøre, fordi dette er den enkleste formen for veiledning. Med denne formen så listes det opp ting som skal gjøres i steg som er enkle å følge. En annen form som ble valgt i noen andre kapitler er å i stedet for å liste opp steg for steg, listes det opp punktvis krav til innhold. Dette har blitt gjort i kapittel der krav til innhold er i fokus og ikke praktiske tiltak.

2.4.7 Design

I veiledningen har leselighet vært første prioritet innenfor design. Det ble fokusert på å ikke ha for lange kapitler, og innenfor disse skulle det være korte avsnitt og gjerne punktvis oppramsing av informasjon som skulle være lette å følge. Oversiktelighet har blitt høyt prioritert i designet, med store entydige overskrifter og ryddige kapitler. For å gjøre veiledningen mer appellerende har det blitt lagt inn sikkerhetsrelaterte sitater i noen kapitler. Vi valgte også å ta med noe skremselspropaganda fra mørketallsundersøkelsen i noen kapitler som ekstra motivasjon for bedriftene. Vi prøvde å bruke så mange illustrasjoner [14] vi kunne, men det var ikke så mange illustrasjoner som kunne brukes. Det ble lagd et flytskjema ut i fra punktene i 'Verdi og trusselvurdering'-kapitlet for å gjøre det mer appellerende. Tallene fra mørketallsundersøkelsen ble også lagt inn i faktabokser. HiG og NorSIS logoene ble brukt på bunnen av dokumentet, dette var også med på å øke helhetsinntrykket av veiledningen.

2.4.8 Innhold i innledning

I innledningen la oppdragsgiver vekt på at det skulle begrunnes hvorfor virksomheter skulle prioritere hendelseshåndtering. Dette skulle vinkles på en slik måte at virksomhetene selv kunne forstå at det er penger å tjene / spare på å ha tilstrekkelig hendelseshåndteringsplaner i bedriften.

Det ble besluttet at den beste strukturen for innledningen på veiledningen ville være å dele den opp i fire forskjellige punkt:

Introduksjon: her blir målgruppen og innholdet i veiledningen kort definert. Det blir nevnt forutsetninger som må være på plass for at virksomhetene skal ha nytte av denne veiledningen, og vi nevner hva virksomhetene bør sitte igjen med etter å ha fulgt veiledningen. På resultatet av å ha fulgt veiledningen valgte vi tre enkle ting; hendelseshåndteringsplaner, hendelseshåndteringspolicy og bedre sikkerhet. Disse tre tingene mener vi virksomhetene bør få etter å ha fulgt veiledningen. Policy og spesielt planer er det denne veiledningen er beregnet på å utvikle, og vi har drevet mye bevisstgjøring rundt sikkerhet gjennom veiledningen, så alle disse tre er realistiske målsetninger for en virksomhet.

Definere og identifisere en sikkerhetshendelse: Vi definerte hva vi la i en sikkerhetshendelse for å gjøre det lettere for virksomhetene som skal bruke veiledningen. I dette punktet beskrev vi en sikkerhetshendelse, det var viktig at vi brukte ordet sikkerhetshendelse om de fleste hendelser som kunne ramme virksomheten, slik at de skjønte at det var et bredt og omfattende begrep. Vi valgte å først legge til grunn en enkel definisjon av en sikkerhetshendelse som flest mulig virksomheter kunne relatere til. Deretter ble det tatt med tre eksempler på sikkerhetshendelser i tre forskjellige typer virksomheter. Dette ble gjort for å nå ut til et større publikum, slik at de som leser veiledningen tenker at dette faktisk gjelder dem. Det ble også definert forskjellen mellom en sikkerhetshendelse og en katastrofe for å unngå forvirring, og for å sette klare rammer for veiledningen.

Hvorfor Hendelseshåndtering?: Dette punktet gikk ut på å motivere bedriftene til å utføre hendelseshåndtering. For å løse dette valgte vi å stille noen spørsmål (hentet fra ROSI-modellen) rundt selve temaet som var rettet mot de som ikke har prioritert hendelseshåndtering før, og de som ikke har noe hendelseshåndtering i det hele tatt. Vi forklarer også litt rundt temaet, blant annet at de fleste virksomheter har hendelser på en daglig basis, og utfordringen ligger ofte i å oppdage disse (eksempel på dette er å installere en brannmur/IDS som logger angrepsforsøk). Dette gjaldt spesielt de som ikke hadde implementert noe som helst form for deteksjonssystemer eller rutiner. De fleste bedrifter bryr seg om omdømmet sitt, vi valgte derfor å bruke dette som et argument for at de burde implementere hendelseshåndteringsplaner.

Når må en hendelse håndteres?: Her ble det brukt en sikkerhetshendelse som eksempel etter ønske fra oppdragsgiver. Her blir det stilt mange spørsmål rundt denne hendelsen, for å legge litt press på leseren og for å få han til å stille de samme spørsmålene rundt sin egen virksomhet. Dette ble også brukt for å motivere leseren til å implementere hendelseshåndteringsplaner.

2.4.9 Innhold i kapitlene

Her beskrives valgene av innhold i hvert kapittel i veiledningen A.

Kapittel 1: Utvikle Hendelseshåndteringspolicy

Ifølge Whitman og Mattord [9] begynner god hendelseshåndteringsplanlegging med en solid policy i bunnen, dette er med andre ord et viktig steg i selve utviklingen av hendelseshåndteringsplaner. Vi baserte oss på NIST 800-34 [8] sin definisjon på hva en god policy skal inneholde, dette er etterprøvd teori så det ble besluttet å ta med mye fra standarden. Minimumskravene til en hendelseshåndteringspolicy ble uthevet med fet skrift i dokumentet. Kravene som ble valgt ut som et absolutt minimum i policyen, er valgt ut med tanke på at det senere skal utvikles gode hendelseshåndteringsplaner ut i fra policyen.

Kapittel 2: Verdi og trusselvurdering (Business Impact Analysis)

Vi anså dette som et av de viktigste kapitlene i veiledningen, fordi det er her virksomhetene selv identifiserer hvilke trusler som er gjeldene. Hensikten med kapittelet ble forklart i en litt lengre innledning, slik at virksomheten skulle få et inntrykk av viktigheten av dette punktet. Det ble lagt vekt på det økonomiske aspektet som ekstra motivasjon til å utføre en slik vurdering.

I selve struktureringen av kapittelet valgte vi en nummerert steg for steg fremgangsmåte. Dette ble fremstilt i et flytskjema for økt leselighet, i tråd med rådene vi fant [15]. Punktene i kapittelet er et absolutt minimum for hva en verdi- og trusselvurdering bør inneholde, vi valgte å veilede gjennom vurderinger av verdier og infrastrukturer, og sikring av disse. Disse valgene ble gjort fordi det var dette vi mente var essensielt å vite før en skal utvikle en god hendelseshåndteringsplan. Det ble diskutert om risikovurdering skulle være med i veiledningen, prosjektgruppens deltagere ville ha med dette, men veileder og oppdragsgiver ønsket ikke å ha det med. Argumentene for å ha det med var at det var en essensiell del i selve business imapct analysis (BIA) delen, og tanken bak var at etter de hadde kjørt en risikovurdering, så kunne de bygge hendelseshåndteringsplaner ut i fra de plausible scenarioene som ble identifisert i BIAen. Argumentene imot dette var at veiledningen ble over en side lengre hvis denne delen var med, og veiledningen skulle være så kortfattig som mulig. Det ble også argumentert for at dette var noe virksomhetene burde ha gjort i forkant av hendelseshåndteringsplan utviklingen, det ble besluttet å utelate informasjon om risikovurdering i veiledningen. I stedet ble det satt som forutsetning for å bruke veiledningen at bedriftene tidligere hadde utført en risikovurdering.

Kapittel 3: Forebyggende tiltak

Oppdragsgiver ønsket et kapittel som inneholdt tekniske sikringstiltak en bedrift kunne innføre. Vi utviklet forebyggende tiltak kapitlet for å få med tiltak virksomhetene bør ha innført. Med dette får vi og definert sikringstiltak som sikkert ikke alle virksomhetene er klar over eksisterer. I kapittelet listes det opp forebyggende og reaktive tiltak som kan innføres for å sikre bedriften mot angrep. Under tekniske tiltak er brannmurer og anitvirusprogrammer listet som et minimumskrav for alle som skal ut på internett. Vi tror at de fleste norske bedrifter har installert

diverse alarmsystemer som fysisk tiltak, men det var greit å nevne det som et eksempel slik at det er klart hva det er snakk om. Rapportsystem er en viktig komponent i hendelseshåndtering, det blir nevnt her for å få ekstra fokus på tiltaket. Oppdragsgiver har ikke avtale med noen antivirus eller brannmur leverandører, så når det skulle foreslås løsninger, ga vi bare eksempler på mange løsninger der prosjektgruppa forbeholder seg nøytrale i forhold til de.

Kapittel 4: Utvikle gjenopprettingsstrategier

Her ble det valgt å forklare 'hvorfor gjenopprettingsstrategier?' ved å vinkle innledningen på det økonomiske aspektet. Selve valgene av hva som har blitt tatt med er minimumskravene vi mener, på bakgrunn av teorien i Whitman og Mattords bok [9], må være på plass i en fungerende gjennopprettingsstrategi. Det ble valgt å legge vekt på rutiner for å ta backup, backup-løsninger, hva, og når virksomhetene skal ta backup. Disse er minimumstiltakene i en gjenopprettingsstrategi.

Kapittel 5: Utvikle en Hendelseshåndteringsplan

Dette er det viktigste punktet i veiledningen. Her valgte vi å bruke en illustrasjon av en enkel hendelseshåndteringsplan tidlig i kapittelet, for å gi leserne et bilde av hvordan en enkel plan kan se ut. Innholdet i dette kapittelet er basert på kravene til en hendelseshåndteringsplan i NIST 800-34 [8]. Vi har listet opp det vi mener er minimumskomponentene til en funksjonell hendelseshåndteringsplan med tanke på kravene til en god hendelseshåndteringsplan:

- Definert omfang.
- Ha en klart definert trigger.
- Klart fordelt ansvar.
- Klart fordelte roller.
- Underretning og kommunikasjon.
- Være klar på hva som er oppgavene til de forskjellige rollene.

Det ble også forklart hva hvert punkt innebar. De punktene som ikke ble uthevet er ikke kritiske for en funksjonell minimumshendelseshåndteringsplan, men det er anbefalt å ha det med i NIST800-34 [8].

Kapittel 6: Øvelser og opplæring

I dette kapittelet ble det avgjort å gå bort fra NIST 800-34 som har veldig tung metodologi for hvordan en skal teste og trene mest mulig effektivt. Det ble for mye teori til å basere dette

kapittelet i veiledningen på standarden, så her ble det valgt å holde seg til et minimum av informasjon. Vi valgte derfor å generelt begrunne hvorfor testing, trening og øving er svært viktig for at virksomhetene skal kunne få maksimalt utbytte av sine planer. Det ble også lagt vekt på bevisstgjøring av de ansatte som en viktig del av det generelle sikkerhetsarbeidet for å få mer fokus på dette området. I avslutningen på kapittelet valgte vi å liste opp fire argumenter for hvorfor øving, testing og trening er svært viktig for effektiviteten av planen. Avslutningen ble formulert på denne måten for å gi virksomhetene ekstra argumentasjon for å gjennomføre disse tiltakene.

Kapittel 7: Vedlikehold av plan

I dette kapittelet valgte vi å kun legge ned noen argumenter for hvorfor vedlikehold er så viktig som det er, og komme med forslag på når det passer å revidere planen. Her valgte vi også å gå litt bort fra standarden [8], og holde oss til et minimum av informasjon. Vi valgte å fokusere på revisjon og anbefale gjennomgang av planer minst en gang i året som et minimum krav.

Kapittel 8: Outsourcing

I dette kapittelet ønsket vi å belyse problematikken rundt outsourcing. Her blir det kommentert på hva virksomheter bør tenke over før de eventuelt leier inn databehandlere. Siden mange virksomheter i dag benytter seg av å outsource tjenester, ønsket vi å belyse aktuelle problemstillinger som det ikke er sikkert alle tenker over før de leier inn databehandlere. Noen av problemstillingene i dette kapittelet hentet vi fra ISO 9001:2008 [16]. ISOen legger vekt på å belyse kvalitet på tjeneste og forventet kvalitet. Vi valgte å ta med dette punktet for at virksomhetene som bruker veiledningen skal være bevisste i sitt valg av databehandler før de eventuelt outsourcer. Et annet viktig punkt som belyses er ansvarsfordeling mellom virksomheten og databehandler, så virksomhetene er klare på hvem som er ansvarlig hvis noe går galt på databehandlers side. Vi ville også belyse problemer rundt å outsource sensitiv informasjon til databehandlere, slik at virksomhetene selv skulle bli bevisste på dette og finne ut av hvordan de skulle takle problemet. Siden dette er en hendelseshåndteringsveiledning, ville vi å belyse problemene rundt hendelseshåndtering når tjenester blir outsourcet. Her valgte vi å legge vekt på rapportering og registrering, for hvis databehandler ikke gjør noen av disse tingene, vil virksomheten aldri få vite om det har skjedd noen hendelser. Databehandleren bør belyse hvilke type angrep virksomheten blir utsatt for, så virksomheten kan ha muligheten til å sikre seg bedre i fremtiden. Vi valgte også å lenke til personopplysningsloven og datatilsynet for å gjøre informasjon rundt temaet mer tilgjengelig.

Kapittel 9: Trusselscenarioer

Dette er et kapittel hvor vi belyser temaer rundt sikkerhet i egen bedrift, her brukte vi ikke noe teori rundt implementering av hendelseshåndtering. Med dette kapittelet ønsket vi å oppnå resonnement rundt egen sikkerhet i virksomhetene som bruker veiledningen. Måten dette ble

gjort på var å liste opp scenarioer, der ett eller flere av scenarione er sannsynlige for de fleste norske virksomheter, og ba virksomhetene stille seg selv disse spørsmålene og svare på scenarionene.

2.4.10 Kvalitetssikring

Prosjektgruppen utviklet veiledningen med tanke på kvalitet, og har grundig kvalitetssikret veiledningen. Etter at kravene til veiledningen ble satt 2.4.3 utifra spørreundersøkelsen og dybdeintervjuene, ble den påbegynt. Den har vært inne til vurdering og diskusjon hos veileder og oppdragsgiver kontinuerlig mens den var under utvikling. Veiledningen ble også sendt ut til en virksomheten NorDoc, for å se om den holdt tilstrekkelig kvalitet. Prosjektgruppen mottok nyttige tilbakemeldinger og forslag til endringer fra bedriften. Finn Olav Sveen, førsteamuensis og foreleser i faget 'Sikkerhetsplanlegging og Hendelseshåndtering' ved HiG, bidro også med innspill til veiledningen.

2.4.11 Tidsbruk og kostnader for å utvikle en hendelseshåndteringsplan

Det var vanskelig å anslå hvor lang tid det vil ta for en virksomhet å utvikle en hendelseshåndteringsplan ved bruk av veiledningen vår. Dette kommer ann på størrelsen og ambisjonsnivået til den individuelle bedriften. Hvis de har svært høyt ambisjonsnivå, og har både tid og penger til å gå i dybden og utenfor rammene i veiledningen vår, så kan utvikling av tilstrekkelige hendelseshåndteringsplaner være en tidkrevende prosess med mye jobb. Hvis de holder seg til minimumskravene vi har satt for utvikling av hendelseshåndteringsplaner, vil det nok ikke ta veldig lang tid. Men dette er vanskelig å anslå, et godt mål på hvor omfattende jobb det vil bli er størrelsen på bedriften og hvor mye kritisk infrastruktur bedriften har. Hvis en risikoanalyse returnerer svært mange sårbarheter som ikke kan sikres med forebyggende tiltak, vil sannsynligvis hendelseshåndteringsplanleggingen ta lang tid. Hendelseshåndtering bør ses på som kontinuerlig arbeid, derfor vil bruk av veiledningen også flettes inn i et kontinuerlig arbeid.

For å gjøre utvikling av hendelseshåndteringsplaner så kostnadseffektivt og attraktivt som mulig, beskriver veiledningen kun minimumstiltak som virksomheter bør utføre i sammenheng med hendelseshåndtering. Ved å legge til lenker til utfyllende materiale i slutten av hvert kapittel, får de som trenger å vite mer om det gitte temaet lett tilgang på ekstra informasjon. Der det har eksistert gode opensource-løsninger, har vi anbefalt disse. Der det ikke fantes noen gode OpenSource produkter, har vi listet opp noen kommersielle alternativer, men det er ikke anbefalt noen av dem.

2.5 Statistikk

Statistikk delen var en av hovedleveransene til prosjektet, og det ble derfor lagt stor vekt på at analysene ble utført på en korrekt måte. Det ble utført korrelasjonsanalyse for spørreundersøkelse og dybdeintervju og ANOVA-analyse for spørreundersøkelse. Fremgangsmåte og metodikk for disse analysene, og annen anvendt metode som er relevant for statistikk blir diskutert i denne seksjonen.

2.5.1 Verktøy

Utførelse av analysene og alle statistiske operasjoner ble utført med statistikk verktøyet R. R er et OpenSource gratis program for statistisk analyse og opprettelse av figurer [17]. For mer informasjon om hvordan R ble brukt, se seksjon 2.6 om skriping i metode.

2.5.2 Målgruppe

Statistikk delen av dokumentet beskriver i hovedsak generell statistikk, og det er ikke ment at leser skal ha stor kunnskap eller erfaring med statistikk. Analysene som er brukt blir forklart i detalj, dette for å sikre at leser har mulighet til å forstå presentert tallmateriale.

2.5.3 Struktur

Statistikk kapitlet ble delt opp i fire seksjoner. Den første omhandlet spørreundersøkelsen, den andre dybdeintervjuet, den tredje diskusjon og den fjerde konklusjoner. Seksjon en og to hadde forholdsvis lik oppbygning. Begge seksjonene inneholdt underseksjoner som beskrev deskriptiv statistikk og korrelasjonsanalyse, mens seksjonen om spørreundersøkelse hadde en ekstra underseksjon om ANOVA-analyse.

Denne struktureringen ble valgt bevisst for å gi god flyt i dokumentet og gjøre det leselig for leseren. Først presenteres generell statistikk for spørreundersøkelsen. Deretter gjøres korrelasjons- og ANOVA-analyse. Deretter kommer dybdeintervjuet, som ble utført etter, og som en fortsettelse på spørreundersøkelsen. Her presenteres først generell statistikk, så korrelasjonsanalyse.

I seksjon tre som omhandler diskusjoner, blir det tatt opp diskusjoner og reflektert over forskningsspørsmålene. Hensikten med denne seksjonen er å diskutere de mest interessante funnene, samt funn som kan benyttes for å belyse forskningsspørsmålene. Strukturen på denne seksjonen er også bevisst valgt. Det presenteres først forskningsspørsmål, deretter funn, slik at leseren raskt får oversikt.

Den siste seksjonen inneholder konklusjonene. Denne har en lik struktur som foregående seksjon,

og presenterer først hypotesene, deretter funnene under hver hypotese. Etter funnene kommer en kort og presis konklusjon på hypotesen. Grunnen til dette er som i forrige seksjon, at teksten skal være oversiktlig og gjøre det enkelt for leseren, samtidig som konklusjonene skal komme klart frem.

2.5.4 Deskriptiv statistikk

Tallmateriale fra spørreundersøkelsen og dybdeintervju ble lagt frem i rapporten under hver sin seksjon om deskriptiv statistikk. *Deskriptiv statistikk er en systematisk organisering og presentasjon av tallmateriale* [18]. I stedet for å presentere standardavvik, konfidensintervall, median, minimumsverdi, maksimumsverdi osv. som man som oftest gjør i deskriptiv statistikk valgte vi å bare presentere resultatene på spørsmålene. Grunnen til dette var at disse var de mest interessante, i tillegg til at rapporten skulle være leselig og forståelig for målgruppen.

2.5.5 Korrelasjonsanalyse

En korrelasjonsanalyse er en analyse som undersøker om det er en lineær sammenheng mellom variablene [3]. I denne sammenheng, kan man undersøke om et spørsmål henger sammen med et annet. For eksempel om det er en sammenheng mellom det å ha opplæring for hendelseshåndtering og om de ansatte vet hva de skal gjøre. Dersom det finnes korrelasjon her, kan man fastslå at det finnes en sammenheng.

Korrelasjonsanalysen benytter verdiene på svaralternativene som inndata. Dette betyr at svaralternativene bør være satt opp på lik måte. Dette var tilfellet på de fleste spørsmålene på spørreundersøkelsen, med et par unntak. Unntakene er beskrevet i vedlegget til korrelasjonsanalysen for spørreundersøkelsen F. På dybdeintervjuene fantes det ingen unntak, her var alle svaralternativene satt opp likt, dvs. fra positiv til negativ.

Korrelasjonsgrad

Når man utfører en korrelasjonsanalyse får man returnert et tall som sier noe om hvor sterk korrelasjonen var, dvs. hvor sterk den lineære sammenhengen er. Gradene av korrelasjon er som følger:

- Veldig svak korrelasjon: 0.0 - 0.2.
- Svak korrelasjon: 0.2 - 0.4.
- Moderat korrelasjon: 0.4 - 0.7.
- Sterk korrelasjon: 0.7 - 0.9
- Veldig sterk korrelasjon: 0.9 - 1.0

Klassifiseringsgradene ble hentet fra [19].

På spørreundersøkelsen ble det tatt med korrelasjoner som hadde korrelasjon over 0.5. På dybdeintervjuet var det færre respondenter og dette gjorde utslag på analysen. Det oppsto derfor flere korrelasjoner. For unngå korrelasjoner som ikke var signifikante i rapporten, økte vi terskelen til 0.7 for dybdeintervjuene.

Positiv og negativ korrelasjon

Det finnes to typer korrelasjon, positiv og negativ:

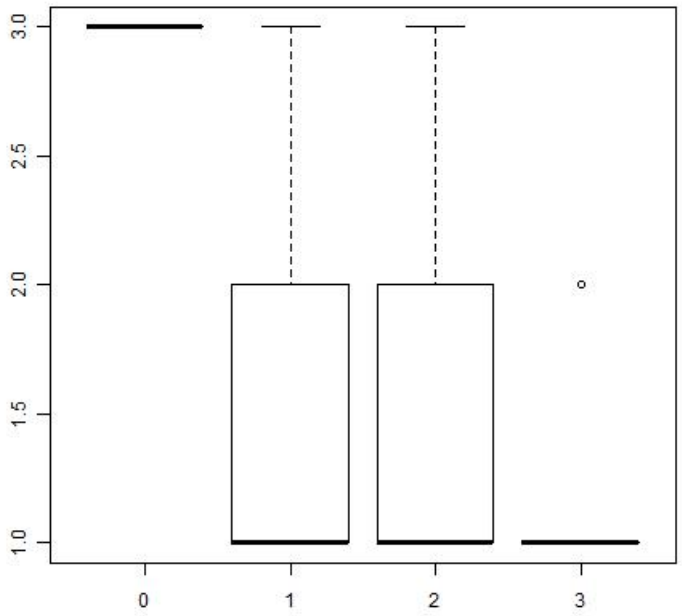
- **Positiv korrelasjon:** Finnes når variablene stiger/synker i takt med hverandre. Dette betyr at når en variabel går opp, går også en annen variabel opp. Et eksempel kan være at dersom virksomheter har mye opplæring innen hendelseshåndtering, vet også ansatte hva de skal gjøre under sikkerhetshendelser.
- **Negativ korrelasjon:** Finnes når variablene stiger/synker i motsatt rekkefølge. Dette betyr at når en variabel går opp, går en annen ned. Et eksempel kan være at dersom virksomheter har god fysisk sikring, så finnes det færre innbrudd.

2.5.6 ANOVA-analyse

ANOVA-analyse står for *analysis of variance* [3]. I en ANOVA-analyse ser man på variasjonen innad i en gruppe og sammenligner dette med variasjonen for alle gruppene. Dersom variasjonen mellom gruppene er betydelig større en variasjonen innad i en gruppe får man utslag. Et eksempel på dette kan være at man sammenligner hvordan ulike sektorer håndterer sikkerhetshendelser. Ved en slik analyse kan man undersøke om en sektor er bedre enn de resterende sektorene.

Man bør ha en god størrelse på utvalget dersom man skal utføre en ANOVA-analyse. Man kan for eksempel ikke si at IT er flinkere enn andre sektorer dersom man bare har et utvalg på tre respondenter. Grunnen til dette er at tre respondenter umulig kan representerer alle, og har man et lavt antall respondenter vil påvirkningskraften til hver respondent øke. Man bør derfor ha et stort utvalg av respondenter dersom man skal utføre en ANOVA-analyse. På grunn av dette valgte vi å ikke utføre ANOVA-analyse på dybdeintervjuene. På spørreundersøkelsen analyserte vi etter størrelse og sektor. For å forsikre oss om at vi fikk stort nok utvalg, brukte vi bare de sektorene som vi hadde flest respondenter, som parametre. Dette var industri, offentlig og IT.

Før man utfører ANOVA-analysen bør man se over med boxplot først. Boxplot lager et plot over et spørsmål, med et annet spørsmål som kategorisk variabel. Dette betyr at man kan vise oversikt over hvordan ulike sektorer svarer på et valgt spørsmål. Eksempel på et boxplot er vist i



Figur 7: Et boxplot eksempel

figur 7. Figuren viser et eksempel over hvordan små, mellomstore og store virksomheter svarte på spørsmålet om de hadde informasjonssikkerhetspolicy. Tallene 1, 2 og 3 horisontalt står for små, mellomstore og store, mens tallene 1, 2 og 3 vertikalt står for ja, nei og vet ikke, dvs. svaralternativene for spørsmålet.

På denne måten kan man se hvordan de ulike virksomhetene har besvart et spørsmål, og om det finnes avvik. Dersom boxplot viser avvik kan man gå videre med å undersøke avviket i en ANOVA-analyse. ANOVA analysen gir et tallresultat. Tar man dette tallet og multipliserer med 100, deretter trekker svaret fra 100 vil man få signifikansen i prosent.

Resultatene som R gir på ANOVA-analysen har følgene oppsett: *Signif. codes: 0:***, 0.001:**, 0.01:*, 0.05:. og 0.1:' '* [17]. Får man signifikans på tre stjerner betyr dette at man kan si med en sikkerhet på 100% at den kategoriske variabelen avviker fra den resterende gruppen. F.eks om en sektor eller størrelse er bedre enn en annen.

2.6 Skripting og automatisering

Statistikkanalysen skulle i så stor grad som mulig være automatisert. Grunnen til dette var at oppdragsgiver ønsket at man enkelt kunne utføre samme undersøkelse i fremtiden for å sammenligne data og se trender. Anvendt metodikk og betraktninger som ble tatt i forhold til dette blir diskutert i denne seksjonen.

2.6.1 Krav

Kravene fra oppdragsgiver var at de skulle kunne utføre spørreundersøkelsen igjen, for å samle inn data og analysere på samme måte som ble gjort i prosjektet. Det statistiske arbeidet ble derfor nødt til å utføres med verktøy hvor en kunne skripte, eller på annen måte automatisere prosessen.

Ut i fra dette ble det satt opp følgende krav til et slikt system:

- Skal være automatisert.
- Skal være enkelt å bruke.
- Skal kunne benyttes i kommende år for samme spørreundersøkelse.
- Skal kunne gi en korrekt statistisk fremstilling og analyse av data.
- Gratis å bruke for oppdragsgiver.

Etter å ha utarbeidet disse kravene, undersøkte vi verktøy for statistikk, samt utviklingsmiljø.

2.6.2 Verktøy

Det finnes mange statistiske verktøy som kan gjøre denne jobben. For å gjøre det statistiske arbeidet så raskt og effektivt som mulig, gjorde vi en liten analyse av hvilke verktøy som passet best til jobben.

Kandidatene var som følger:

- Excel. Et stort kommersielt program for blant annet regneoperasjoner og fremvisning av grafer [20].
- SPSS. Et kommersielt program for statistisk analyse og opprettelse av figurer [21].
- R. Et OpenSource gratis program for statistisk analyse og opprettelse av figurer [17].

Excel

Excel var det programmet vi hadde mest kjennskap til og kunne best. Selv om dette var kommersielt, så var vi allerede i besittelse av denne applikasjonen og dette var et reelt alternativ. Allikevel så er ikke Excel en applikasjon for statistikk. Det finnes funksjonalitet og grafer, men mangler innebygde funksjoner for å gjøre de analysene vi var ute etter. Ettersom vi hadde store krav til det statistiske arbeidet, valgte vi å forkaste Excel som alternativ.

SPSS

SPSS hadde vi ingen kjennskap til før prosjektet. Allikevel er det dette programmet som benyttes mest til statistiske analyser. Dette programmet er veldig brukervennlig og har stor funksjonalitet. En brukerlisens for studenter er ikke veldig dyr, og vi vurderte sterkt å benytte dette programmet. Men vi måtte også sørge for at oppdragsgiver kunne bruke skriptene vi utviklet. Siden oppdragsgiver ikke hadde SPSS, og SPSS koster 16.600,- deretter 4.300,- for årlig lisens valgte vi å ikke benytte dette verktøyet, ettersom vi ikke ønsket å låse oppdragsgiver til et produkt med høye kostnader.

R

R er et OpenSource verktøy for analyse av statistikk. Det er et kommandolinjeverktøy og forholdsvis tungt å bruke. Vi hadde ingen kjennskap til R før prosjektet. Til tross for dette så er R et strålende statistisk verktøy som gir korrekte statistiske analyser og har gode muligheter til skripting og automatisering. I tillegg til dette er det gratis. Allikevel var vi usikre på om dette var riktig verktøy for oss, ettersom det bruker et eget kodespråk og det tar tid å sette seg inn i dette. Heldigvis for oss hadde veileder stor kunnskap og god erfaring med verktøyet, og oppfordret oss til å bruke det. Vi valgte derfor å benytte R som verktøy for statistisk analyse.

2.6.3 Utviklingsmiljø

Etter å ha valgt verktøy undersøkte vi hvordan vi kunne levere produktet til oppdragsgiver slik at skriptene på enklest mulig måte kunne tas i bruk. Vi fant to potensielle løsninger på dette, den første var å utvikle instruksjoner for bruk av skript, den andre var å levere en virtuell maskin med skriptene på. Løsningene er diskutert under:

- **Skript med instruksjoner:** Tanken her var å skrive skriptene ferdig og levere disse elektronisk sammen med instruksjoner for bruk. Instruksjonene måtte da ha inneholdt instruksjoner for installering av valgt verktøy, samtidig som plassering av skript og inndata filer måtte vært beskrevet i stor detalj slik at skriptene ville fungert. Dette ville vært den enkleste løsningen

for oss, men dette legger arbeidet på oppdragsgiver, noe vi ikke ønsket.

- **Virtuell maskin:** Tanken her var å opprette en virtuell maskin hvor vi installerte verktøy og utviklet skriptene ferdig slik at oppdragsgiver bare kunne starte maskinen i et virtuelt miljø, deretter kjøre skript. Denne løsningen er enkel, samtidig som den gjør arbeidet for oppdragsgiver mindre.

På bakgrunn av dette valgte vi virtuell maskin som løsning.

Krav til virtuell maskin

For levere denne løsningen valgte vi å sette opp noen krav til den virtuelle maskinen. Vi ønsket en løsning som var enkel å implementere, men samtidig enkel å arbeide med. For å oppnå dette ble valget av operativsystem og størrelse på disk det viktigste for løsningen.

Siden valget av operativsystem direkte påvirker hvor enkel løsningen er å bruke og hvor stor diskplass som blir brukt, er dette det viktigste punktet. Velger man Windows får man et brukergrensesnitt som de fleste er kjent med og klarer å bruke. Dette setter derimot store krav til diskplass, ettersom Windows installasjoner bruker ca. 20GB. I tillegg må man gå til innkjøp av lisens. Siden vi ønsket å levere den virtuelle maskinen på en liten og rimelig minnepinne var dette uaktuelt. Et annet alternativ var å bruke en Linux distribusjon. Grunnen til dette er at disse har et godt brukergrensesnitt, i tillegg til at de bruker lite diskplass. Valget sto derfor mellom å bruke Debian eller Ubuntu, siden det var disse vi var mest kjent med. Valget var allikevel forholdsvis enkelt ettersom vi måte ha et brukergrensesnitt som var enkelt å forholde seg til. Dette har Ubuntu. Valget falt derfor på Ubuntu.

Vi endte dermed opp med et OpenSource operativsystem, med OpenSource verktøy. Vi oppfylte kravet om et enkelt brukergrensesnitt, samtidig som krav til diskplass ble forholdsvis lite (4GB). I tillegg til dette så ble eneste kostnad innkjøp av minnepinne.

2.6.4 Skript og kode

For å helautomatisere statistikken ble det valgt at all analyse skulle skrives i skript, slik at oppdragsgiver ved å utføre en kommando kunne utføre samme analyse.

Måten vi valgte å løse dette på var å skrive skript filer for R, samt et bash skript for å starte de skriptene som måtte kjøres. Men før dette så måtte data hentes fra Questback som var verktøyet som ble brukt for spørreundersøkelsen. Dessverre så hadde ikke Questback et format for eksportering av data som passet for R. Det ble derfor nødvendig å skrive et vaskeprogram for å omstrukturere dataene på en slik måte at R kunne lese dem.

Vaskeprogram

For å utføre omstruktureringen av data var det nødvendig å skrive et skript eller program som tok inndata fra Questback og gjorde det om til inndata som R kunne håndtere. For å gjennomføre dette kodet vi et C++ program i g++ [22]. Grunnen til at vi benyttet C++ var fordi det var dette vi hadde mest kjennskap til. I tillegg til dette så er det enkelt å skrive et program i g++ som kan kjøres som en del av et skript.

Kravene som ble stilt til et slikt system var at det skulle:

- Lese data fra Questback rapport.
- Skrive data til fil som kan leses av R.
- Fungere likt uansett hvor mange respondenter.

Siden det er flere måter å hente ut en Questback rapport, måtte det gjøres noen forutsetninger i metoden dette ble gjort på for at vaskeprogrammet skal fungere. Disse forutsetningene var at:

- Rapporten må hentes ut som rådata fil i .csv format.
- Rapporten må hentes med tabulator som feltseparator og dataverdier i tallformat.
- Rapporten må navnes om til data.csv.

For at inndatafilen skal kunne leses av R må alle kommentarer fjernes og bare tall være oppført. Dette betyr at vaskeprogrammet må fjerne all unødvendig tekst som rapporten genererer.

For å få vaskeprogrammet til å fungere uansett antall respondenter måtte vaskeprogrammet tilpasses slik at det ikke leser en fast lengde, men leser til det ikke finnes fler respondenter.

Vaskeprogrammet som ble skrevet oppfyller alle disse kravene så lenge forutsetningene ovenfor blir fulgt. Vaskeprogrammet er lagt ved som vedlegg sammen med de andre skriptene J.

R Skript

R er et verktøy som har et eget kodespråk og kompilator. Koding i R minner mye om bash skript, men har selvfølgelig egne syntakser og kommandoer. I tillegg finnes det mange tilleggspakker som gir ekstra funksjonalitet dersom dette er nødvendig. Vi skrev tre skript for R. Et som lager barplot for spørreundersøkelse og dybdeintervju, et som utfører korrelasjonsanalyse og et som utfører anova analyse. Skriptet som lager barplot kan kjøres automatisk og oppretter bildefiler med barplot uten at noen form for brukerinteraksjon er nødvendig. Korrelasjonsskriptet kan og kjøres automatisk, dette skriver ut de spørsmålene som hadde korrelasjon over 0.5. Skriptet

for ANOVA-analysen derimot kan ikke automatiseres, ettersom dette krever at bruker gjør en vurdering etter å ha sett over boxplot, før man utfører anova analysen. Skriptet vi laget for ANOVA-analysen ble allikevel lagt med, slik at oppdragsgiver kan bruke koden som et eksempel. R skriptene er lagt ved som vedlegg sammen med de andre skriptene J.

Bash Skript

Bash skriptet er skriptet som knytter alle skriptene sammen. Dette er et enkelt skript som først kjører vaskeprogrammet, deretter kjøres R skript som oppretter bilder med barplot, samt korrelasjonsanalysen. Se vedlegg J.

Instruksjoner for kjøring av skriptene er lagt ved i filen Instruksjoner.txt som ligger på skrivebordet på den virtuelle maskinen.

2.6.5 Testing og kvalitetssikring

For å sikre at skriptene fungerte slik de skulle, var det nødvendig med omfattende testing. Grunnen til dette var at vi ønsket at skriptene skulle kjøre likt hver gang, og levere korrekte statistiske data og analyser.

Det å få skriptene til å kjøre likt hver gang burde ikke være noe problem. Allikevel kan det oppstå problemer, siden skriptene bruker forskjellige datafiler som inndata hver gang det kjøres. Dette problemet ble godt løst vha. vaskeprogrammet som ble utviklet. Takket være dette programmet har all inndata lik struktur, og skriptingen i R trenger ikke ta høyde for alle mulige situasjoner, men en forutbestemt struktur. Forutsigbarhet ble derfor ikke noe problem, og testingen av dette var ikke tidkrevende.

Siden vi valgte statistikk verktøyet R for å utføre de statistiske operasjonene fryktet vi ikke at skriptene ville gi feil informasjon. Så lenge riktige parametre og verdier ble brukt, var det ingen fare for at R skulle gi feil informasjon. Dette kravet ble dermed forholdsvis enkelt å oppfylle, så lenge skriptene ble kodet korrekt.

2.6.6 Nytteverdi

Tiltakene som ble beskrevet ovenfor førte til at skriptene ble helautomatiserte, kjørte likt hver gang og ga korrekte statistiske data. Automatiseringen av statistikken har en rekke fordeler. Disse er blant annet at oppdragsgiver vil ha mulighet til å utføre den samme undersøkelsen senere, samt at den vil bli utført på samme måte. Dette gir god mulighet til å se trender hos norske SMBer om hvordan hendelseshåndtering anvendes. Man kan da utføre en undersøkelse hvert år, se hvordan situasjonen forandrer seg, hva som fungerer bra og hvor det er størst forbedringspoten-

siale. Dette kan danne et viktig informasjonsgrunnlag for videre undersøkelser og kunnskap om hendelseshåndtering i norske SMBer, siden dette etter vår kunnskap og litteraturundersøkelse, ikke eksisterer fra før.

3 Statistikk

Hensikten med denne oppgaven er å kartlegge hvordan norske virksomheter bedriver hendelseshåndtering. Vi ønsket ikke bare å samle generell statistikk på temaet, men også besvare hypotesene som er satt opp, slik at vi kan si noe om hvordan situasjonen er i norske virksomheter. Bortsett fra noen unntak [23–25], så er det ikke utført mange undersøkelser på dette emnet, og spesielt ikke rettet mot norske SMBer. Det er derfor interessant å undersøkelse dette emnet, og vi håper med denne delen av oppgaven å bidra til å øke forståelsen og kunnskapen om hendelseshåndtering i Norske SMBer.

Dette kapitlet består av spørreundersøkelsen og dybdeintervjuet som ble utført for å oppnå målene beskrevet ovenfor. Først kommer det en seksjon med spørreundersøkelse hvor det blir beskrevet deskriptiv statistikk, deretter korrelasjonsanalysen og ANOVA-analysen. Neste seksjon omhandler dybdeintervju. Her presenteres deskriptiv statistikk og korrelasjonsanalyse. Ingen ANOVA-analyse ble utført her, ettersom utvalget var noe mindre for dybdeintervjuet. Til slutt i kapitlet kommer en seksjon med diskusjon, hvor det blir tatt opp diskusjoner og reflektert over forskningsspørsmålene og hypotesene. Kapitlet avslutter med en konklusjon, som konkluderer og gir svar på hypotesene som ble satt opp i seksjon 1.8.

3.1 Spørreundersøkelse

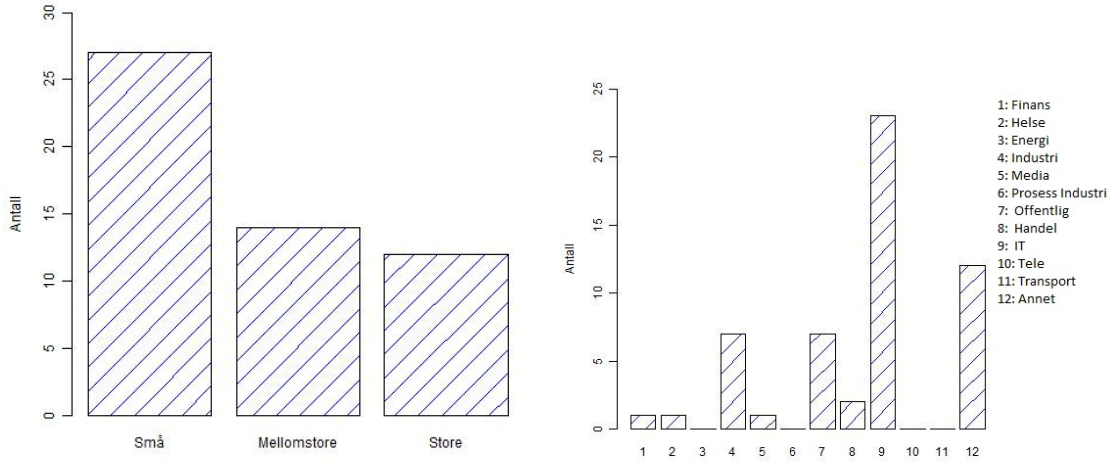
Som nevnt i seksjon 2.1.2 om metodikk, så ble spørreundersøkelse og dybdeintervjuer valgt som fremgangsmåte for å besvare hypotesene som ble satt opp til forskningsspørsmålene.

3.1.1 Deskriptiv statistikk

Spørreundersøkelsen ble satt opp på en slik måte at den skulle besvare mesteparten av hypotesene, men samtidig være liten nok til at vi fikk stor nok svarprosent. Undersøkelsen besto av 23 spørsmål, og ble sendt ut til 148 virksomheter, hvorav 54 stykker svarte. Dette er en svarprosent som tilsvarer 36%. Spørreundersøkelsen er lagt ved som vedlegg B.

Om respondentene

Av respondentene så var 51% fra små, 26% fra mellomstore og 23% fra store virksomheter. Oversikt over virksomhetene etter størrelse kan du se i figur 8.a. Ettersom det i hovedsak er små og



(a) Størrelse

(b) Sektor

Figur 8: Figur A viser virksomheter etter størrelse, mens figur B viser virksomhet etter sektor

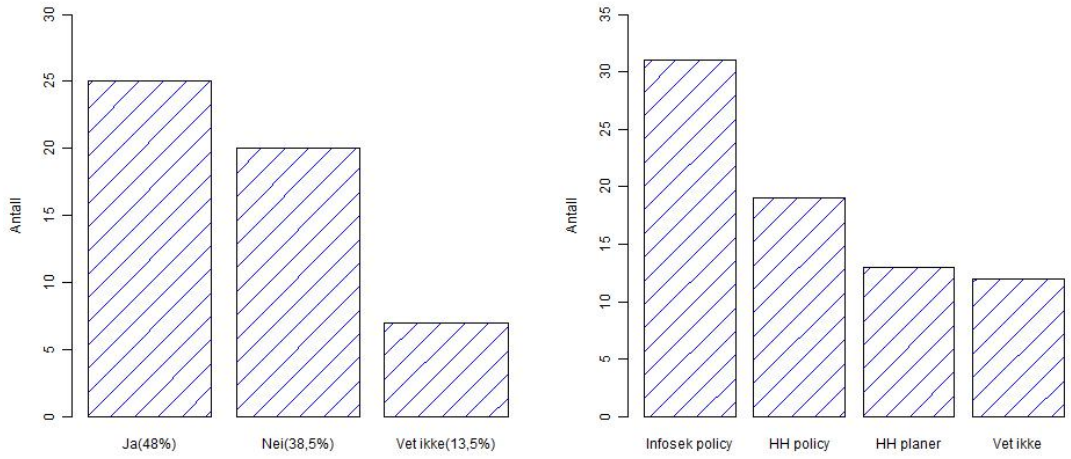
mellomstore virksomheter som er målgruppen til oppdragsgiver, var det viktig for oss å få nok respondenter fra disse, slik at vi fikk et representativt utvalg. Selv om undersøkelsen i hovedsak dreier seg om SMB, tok vi med noen store bedrifter, for statistisk data til sammenligning. Vi ønsket i tillegg å få informasjon om hva de store virksomhetene gjør innenfor hendelseshåndtering og hvor godt dette fungerer. Figur 8.b viser oversikten over hvilken sektor de forskjellige respondentene kommer fra. 23 respondenter kommer fra IT, dette tilsvarer 43%. Grunnen til at dette tallet er så høyt er pga. at listen er hentet fra kontaktlisten til NorSIS, som nevnt i seksjon 2.2.8 om metodikk. Ettersom antallet respondenter fra IT er såpass høyt, kan IT sammenlignes opp mot norske bedrifter generelt, for å se om IT er flinkere eller dårligere på hendelseshåndtering. Det ble også tatt med respondenter fra offentlig virksomhet, fordi vi ønsket å sammenligne offentlige virksomheter opp mot private.

Policy

Informasjonssikkerhetspolicy og hendelseshåndteringspolicy er nødvendige generelle dokumenter som danner grunnlaget for videre arbeid med informasjonssikkerhet og hendelseshåndtering. Det er derfor viktig å få kartlagt hvor mange norske virksomheter som har utviklet disse, og hvordan de blir brukt. Vi spurte totalt fire spørsmål om bruk av policy.

68% svarte at de hadde informasjonssikkerhetspolicy. 26% svarte nei, mens 6% svarte vet ikke.

Når spurt om denne dekket hendelseshåndtering, svarte 51% av respondentene ja, 37% nei og 12% vet ikke. Omlag 49% av virksomhetene svarte at de hadde egen hendelseshåndteringspolicy.



(a) Definert sikkerhetshendelse

(b) Gjennomgår i opplæringen

Figur 9: fig:Figur A viser definert sikkerhetshendelse, figur B viser hva virksomhetene går gjennom under opplæring

52% av virksomhetene svarte nei eller vet ikke når spurt om sikkerhetshendelse var definert i informasjonssikkerhetspolicy eller hendelseshåndteringspolicy. Oversikt vist i figur 9.a.

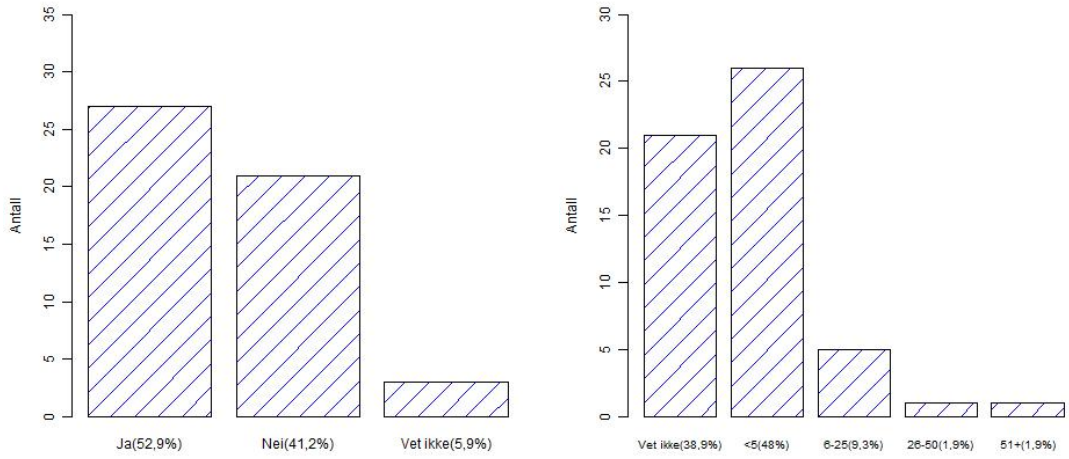
Opplæring

Som kjent, så er sikkerheten kun like god som det svakeste leddet. Og det svakeste leddet er som oftest mennesket [26]. Det er derfor viktig at virksomhetene har gode opplæringsrutiner, slik at mange sikkerhetshendelser hindres i å oppstå, eller håndteres på en god måte. Vi spurte tre spørsmål om hvordan virksomhetene benytter opplæring.

Vi spurte om virksomhetene hadde gjennomgang av informasjonssikkerhetspolicy, hendelseshåndteringspolicy og hendelseshåndteringsplaner under opplæring. Som figur 9.b viser så hadde 31 virksomheter(57%) gjennomgang av informasjonssikkerhetspolicy under opplæring. 19 virksomheter (35%) har gjennomgang av hendelseshåndteringspolicy under opplæring. 13 virksomheter (24%) har gjennomgang av hendelseshåndteringsplaner under opplæring.

Når det kom til opplæring for ledelsen, svarte omlag 35% at de hadde opplæring vedrørende hendelseshåndtering for ledelsen.

Ved spørsmålet som omfattet gjennomføring av øvelser, hadde 24% gjennomført øvelser basert på hendelseshåndteringsplanene.



(a) Rutiner for rapportering

(b) Antall registrerte sikkerhetshendelser

Figur 10: Figur A viser barplot av rutiner for rapportering, mens figur B viser barplot av antall registrerte sikkerhetshendelser

Registrering og rapportering

Registrering av sikkerhetshendelser er en nødvendighet for alle virksomheter. Dersom man ikke registrerer sikkerhetshendelser, kan man umulig vite hvilke angrep som rammer bedriften, og hvilke trusler man står ovenfor. Rapportering til ledelse er også viktig, ettersom det er ledelsen som må ta ansvar for at planer og rutiner blir opprettet og fulgt. En tidligere undersøkelse [24], viser at et flertall av norske virksomheter ikke har implementert tekniske verktøy som IDS for å oppdage sikkerhetshendelser. Undersøkelsen viste også at flertallet ikke hadde rutiner for å rapportere sikkerhetshendelser. Vi spurte syv spørsmål om hvilke rutiner virksomhetene hadde for registrering og rapportering.

Som figur 10.a viser så har bare 30 virksomheter (53%) rutiner for å varsle, eller rapportere sikkerhetshendelser.

Når det ble spurt om muligheter for anonym rapportering av sikkerhetshendelser, svarte 23% at de hadde dette.

Dersom det skulle oppstå en sikkerhetshendelse svarte 83% at de vet hvem de skal kontakte.

75% svarte at det er klare rutiner på plass dersom det er behov for ekstern kontakt under en sikkerhetshendelse, som for eksempel kontakt med politi, ambulanse, brannvesen o.l..

Figur 10.b viser et barplot over antall sikkerhetshendelser som ble registrert hos virksomhetene i 2009. Som figuren viser så svarte hele 39% at de ikke vet hvor mange sikkerhetshendelser som ble registrert i 2009.

Når spurt om hvor mange av disse som ble rapportert videre til ledelsen, så var resultatet det samme. Dvs. at alle registrerte sikkerhetshendelser i 2009 ble rapportert videre til ledelsen.

Hele 42% svarte nei eller vet ikke, når spurt om det fantes noen form for IDS for å oppdage tekniske sikkerhetshendelser.

Hendelseshåndtering

Denne delen av spørreundersøkelsen består av spørsmål som omfatter rutiner for hendelseshåndtering. Vi spurte seks spørsmål om rutiner for hendelseshåndtering. Dette innebærte generelle spørsmål om hendelseshåndtering, og spørsmål om verdi og trussel analyse. Det ble kun tatt med generelle spørsmål om hendelseshåndtering i denne spørreundersøkelsen, for mer grundig analyse om hendelseshåndteringsplaner og rutiner, se seksjon 3.2.1 under dybdeintervju. Grunnen til at vi spurte om, og syntes verdi og trusselanalyse er viktig, er fordi dette danner grunnlaget for videre arbeid med hendelseshåndtering. Dette gir virksomheter større innsikt i hvilke verdier de har, og hvilke trusler de står ovenfor.

37% av respondentene svarte at de hadde satt av midler til hendelseshåndtering.

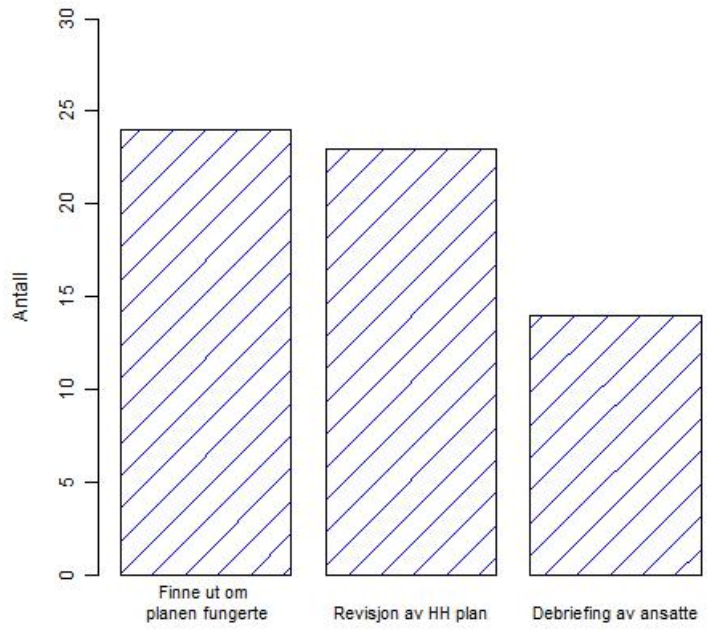
64% svarte at de hadde dedikert personell som håndterer sikkerhetshendelser.

Vi sjekket også hvilke rutiner virksomhetene hadde etter endt sikkerhetshendelse. Se figur 11. 24 respondenter(44%) svarte at de hadde rutiner for å finne ut om hendelseshåndteringsplanen fungerte etter en endt sikkerhetshendelse. 23 respondenter(43%) svarte at de hadde revisjon av hendelseshåndteringsplan etter endt sikkerhetshendelse. Mens 14(26%) svarte at de hadde debriefing av ansatte etter endt sikkerhetshendelse.

69% svarte at de hadde rutiner for å vurdere risikoer virksomheten sto ovenfor. 24% svarte nei, og 7% vet ikke.

Når respondentene ble spurt om de hadde rutiner for å vurdere verdiene til virksomheten derimot, svarte bare 54% at de hadde dette. 27% svarte nei, og 19% vet ikke.

44% hadde beskrevet konsekvenser for de ansatte, dersom sikkerhetsregler/policy blir brutt.



Figur 11: SU Barplot Rutiner etter endt sikkerhetshendelse

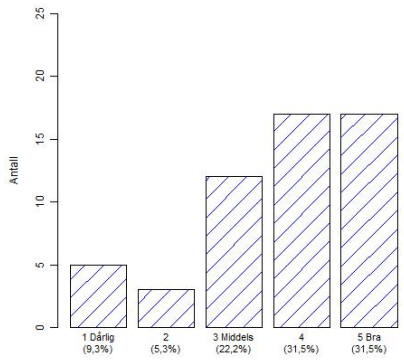
Case

Til slutt i spørreundersøkelsen ga vi et case. Caset var som følgende: ”Dersom din virksomhet blir utsatt for et angrep som er av en slik alvorlighetsgrad at det må håndteres...’ .

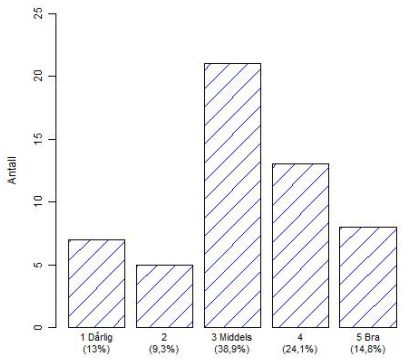
Som figur 12.a viser, så har de fleste troen på seg selv. 63% tror de kommer til å håndtere sikkerhetshendelsen over middels til bra. Figur 12.b viser oversikt over hvor godt respondentene tror medarbeideren kommer til å håndtere sikkerhetshendelsen. 22% av respondentene mener at medarbeiderne kommer til å håndtere sikkerhetshendelsen dårlig. Figur 12.c viser hvordan respondentene tror virksomheten kommer til å håndtere sikkerhetshendelsen. Som figuren viser, så tror de fleste respondentene at virksomheten vil håndtere sikkerhetshendelsen godt.

3.1.2 Korrelasjonsanalyse

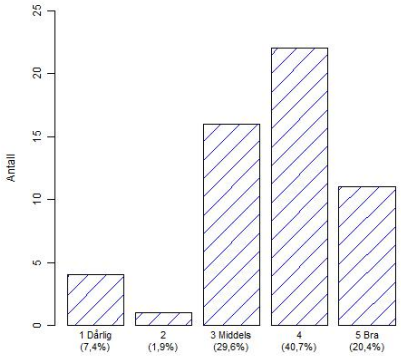
Korrelasjonsanalysen undersøker om det finnes lineære sammenhenger mellom spørsmålene. Dette ble beskrevet i seksjon 2.5.5 om metode for statistikk. I analysen undersøkte vi om spørsmålene har positiv korrelasjon over 0.5 eller negativ korrelasjon under -0.5.



(a) CaseDu



(b) CaseMedarbeider



(c) CaseVirksomheten

Figur 12: Figur A viser hvor godt respondent tror han/hun, figur B hvor godt medarbeiderne, figur C hvor godt virksomheten vil håndtere sikkerhetshendelsen

Denne seksjonen beskriver de mest interessante funnene av korrelasjonsanalysen. Korrelasjonene er først listet opp i en tabell, deretter diskutert. For en oversikt over hele analysen, se vedlegg F.

De tre siste spørsmålsparene i tabell 1, har svaralternativer som er satt opp motsatt. Dvs. at positive svaralternativer har motsatt rekkefølge hos spørsmålene. Det er dermed ikke negativ korrelasjon for disse, men positiv.

Policy

Korrelasjonsanalysen viste at det fantes korrelasjon mellom spørsmålet om hendelseshåndteringspolicy og informasjonssikkerhetspolicy. Dvs. at har man informasjonssikkerhetspolicy, så har

Tabell 1: Tabell over viktigste korrelasjoner fra spørreundersøkelsen.

Spørsmålspar	**Korrelasjon**
'Hvor mange sikkerhetshendelser ble registrert i din virksomhet i 2009?' og 'Hvor mange av de registrerte hendelsene ble rapportert videre til ledelsen?'	0.87
'Dekker denne policyen hendelseshåndtering?' og 'Beskriver informasjonssikkerhetspolicyen eller hendelseshåndteringspolicyen hva en sikkerhetshendelse er?'	0.81
'I hvor stor grad vet du hva du skal gjøre?' og 'Hvor godt tror du virksomheten i sin helhet kommer til å håndtere hendelsen?'	0.79
'I hvor stor grad tror du at medarbeiderne dine vet hva de skal gjøre?' og 'Hvor godt tror du virksomheten i sin helhet kommer til å håndtere hendelsen?'	0.79
'Har virksomheten noen rutiner for å finne ut om hendelseshåndteringsplanen fungerte?' og 'Har virksomheten rutiner for revisjon av hendelseshåndteringsplan?'	0.78
'Har virksomheten rutiner for revisjon av hendelseshåndteringsplan?' og 'Har virksomheten rutiner for debriefing av ansatte?'	0.77
'I hvor stor grad vet du hva du skal gjøre?' og 'I hvor stor grad tror du at medarbeiderne dine vet hva de skal gjøre?'	0.75
'Har din virksomhet en informasjonssikkerhetspolicy?' og 'Har din virksomhet en egen hendelseshåndteringspolicy?'	0.63
'Dekker denne policyen hendelseshåndtering?' og 'Har din virksomhet en egen hendelseshåndteringspolicy?'	0.6
'Har virksomheten noen rutiner for å finne ut om hendelseshåndteringsplanen fungerte?' og 'Har virksomheten rutiner for debriefing av ansatte?'	0.59
'Går dere gjennom informasjonssikkerhetspolicy som en del av opplæringen' og 'I hvor stor grad vet du hva du skal gjøre?'	0.56
'Har din virksomhet en informasjonssikkerhetspolicy?' og 'Beskriver informasjonssikkerhetspolicyen eller hendelseshåndteringspolicyen hva en sikkerhetshendelse er?'	0.55
'Har virksomheten kursing / opplæring vedrørende hendelseshåndtering for ledelsen?' og 'Har virksomheten rutiner for debriefing av ansatte?'	0.54
'Har din virksomhet en egen hendelseshåndteringspolicy?' og 'Beskriver informasjonssikkerhetspolicyen eller hendelseshåndteringspolicyen hva en sikkerhetshendelse er?'	0.52
'Har virksomheten kursing / opplæring vedrørende hendelseshåndtering for ledelsen?' og 'Utfører virksomheten øvelser basert på hendelseshåndteringsplanene?'	0.52
'Har din virksomhet en informasjonssikkerhetspolicy?' og 'Har dere gjennomgang av informasjonssikkerhetspolicy som en del av opplæringen?'	-0.61
'Har din virksomhet en egen hendelseshåndteringspolicy?' og 'Har dere gjennomgang av informasjonssikkerhetspolicy som en del av opplæringen?'	-0.59
'Har din virksomhet en egen hendelseshåndteringspolicy?' og 'Har dere gjennomgang av hendelseshåndteringspolicy som en del av opplæringen?'	-0.51

man som oftest også hendelseshåndteringspolicy.

Analysen viste også at det fantes korrelasjon mellom hendelseshåndteringspolicy og spørsmål angående opplæring for informasjonssikkerhetspolicy og hendelseshåndteringspolicy. Dvs. at dersom en virksomhet har hendelseshåndteringspolicy, så har man også opplæring for informasjonssikkerhetspolicy eller hendelseshåndteringspolicy. Dette viser at dersom man utvikler hendelseshåndteringspolicy, settes det og et større fokus på opplæring i virksomheten. Eller motsatt, dvs. at mangel på hendelseshåndteringspolicy, fører til at man ikke har opplæring.

Det viste seg også å være svak korrelasjon mellom spørsmålene om virksomheten hadde informasjonssikkerhetspolicy og hendelseshåndteringspolicy, og om sikkerhetshendelse er definert. Dette betyr at dersom virksomhetene har policy som dekker informasjonssikkerhet eller hendelseshåndtering, så er også sikkerhetshendelse definert. Spørsmålet om informasjonssikkerhetspolicy dekket hendelseshåndtering og om sikkerhetshendelse var definert hadde også korrelasjon.

Opplæring

Analysen av spørsmålet om virksomheten hadde opplæring av informasjonssikkerhetspolicy viste at det fantes svak korrelasjon med spørsmålet om ansatte visste hva de skulle gjøre under en sikkerhetshendelse. Dette beviser at dersom man utfører opplæring om informasjonssikkerhetspolicy, så vet også de ansatte hva de skal gjøre. Med andre ord, opplæring fungerer.

Opplæring for ledelsen

Analysen resulterte i to tilfeller av korrelasjon tilknyttet spørsmålet om opplæring for ledelsen. Den ene korrelasjonen var mellom spørsmålet for opplæring for ledelse og øvelser basert på hendelseshåndtering. Den andre korrelasjonen var mellom opplæring for ledelse og om det fantes debriefing for ansatte. Øvelser basert på hendelseshåndtering er viktig for at ansatte skal kunne reagere riktig og håndtere sikkerhetshendelsen godt, mens debriefing av ansatte kan være viktig å gjennomføre for at ansatte skal få ro etter sikkerhetshendelsen, i tillegg å lære av det som skjedde. Begge disse hadde svak korrelasjon med opplæring av ledelsen, dette viser at to viktige aspekter i hendelseshåndtering øker/synker lineært sammen med opplæring for ledelsen. Altså, hvis ledelsen har hatt opplæring innenfor hendelseshåndtering, er sannsynligheten for at virksomheten har gode rutiner for øvelser og debriefing større.

Registrering og rapportering

Analysen viste at det var sterk korrelasjon mellom spørsmålet om hvor mange sikkerhetshendelser som ble registrert i 2009, og hvor mange av disse som ble rapportert videre til ledelsen. Dette er veldig bra, og viser at dersom de som har implementert rutiner for å registrere sikker-

hetshendelser også rapporterer disse videre til ledelsen.

Etter endt sikkerhetshendelse

Vi spurte tre spørsmål om rutiner etter endt sikkerhetshendelse. Disse var som følgende:

- Har virksomheten noen rutiner for å finne ut om hendelseshåndteringsplanen fungerte?
- Har virksomheten rutiner for revisjon av hendelseshåndteringsplan?
- Har virksomheten rutiner for debriefing av ansatte?

Disse spørsmålene hadde gjensidig korrelasjon, dvs. at alle spørsmålene stiger/synker i takt. Og virksomhetene som har rutiner etter endt sikkerhetshendelse, som oftest har implementert alle tre.

Case

De tre spørsmålene som dekket case, om hvor godt respondenten selv, medarbeideren og virksomheten ville håndtere sikkerhetshendelsen, viste analysen at det var gjensidig korrelasjon. Dvs. at alle spørsmålene stiger og synker i takt.

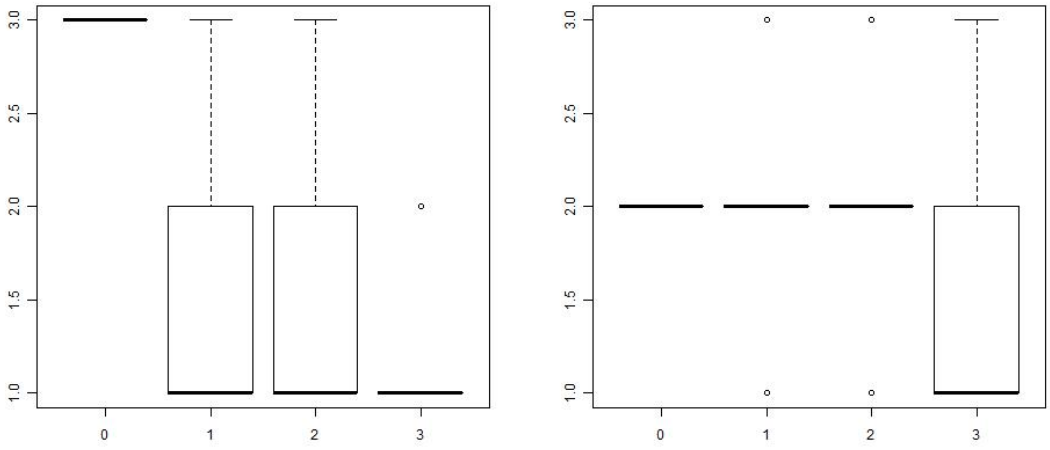
3.1.3 ANOVA-analyse

I denne seksjonen har vi analysert om det finnes forskjell mellom ulike grupper på de forskjellige spørsmålene. Dvs. at vi kan velge virksomheter etter sektor eller størrelse, og se hvordan disse er i forhold til resten. Analysen vi har utført tok for seg forskjeller mellom små, mellomstore og store virksomheter og hvordan industri, offentlig og IT avviker fra andre virksomheter. Grunnen til at vi bare analyserte disse sektorene, var fordi vi ikke hadde nok respondenter fra de andre sektorene. Vi ønsket at gruppene vi analyserte hadde over 10% av det totale antallet, dvs. at det var nok respondenter for å gjøre en slik analyse.

Analyse etter størrelse

Analysen vi gjorde etter størrelse, viste at i alle tilfeller hvor det fantes signifikante avvik(signifikans over 90%), så var store virksomheter var flinkere. Det er her tatt med et utdrag fra analysen. For hele resultatet av ANOVA-analysen, se vedlegg G.

Figur 13.a viser et boxplot over spørsmålet om hvor mange som har informasjonssikkerhetspolicy. Tallene 1, 2 og 3 horisontalt står for små, mellomstore og store, mens tallene 1, 2 og 3 vertikalt står for ja, nei og vet ikke, dvs. svaralternativene for spørsmålet. Som figuren viser



(a) Boxplot infosekpolicy

(b) Boxplot øvelse

Figur 13: Figur A viser boxplot over hvor mange som har informasjonssikkerhetspolicy, mens figur B viser øvelser basert på hendelseshåndteringsplanene

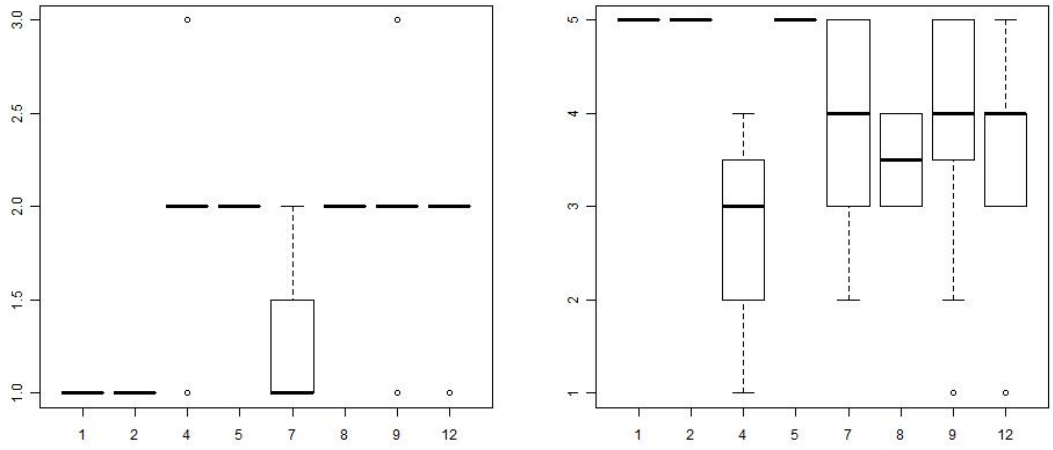
så er store virksomheter flinkere på å ha informasjonssikkerhetspolicy. Dette bekrefter ANOVA-analysen, med en signifikans på 94,4%. Figur 13.b viser et boxplot over spørsmålet om hvor mange virksomheter som har øvelser basert på hendelseshåndteringsplanene. Tallene er satt opp på lik måte som i figur A. Som figuren viser så er små og mellomstore virksomheter vesentlig dårligere på dette. Dette bekreftet ANOVA-analysen med en signifikans på 97,7%.

Analysen viste også at store virksomheter var flinke til å definere sikkerhetshendelse, samt rutiner for anonym rapportering.

Analyse etter sektor

Analysen vi gjorde etter sektor, viste at offentlig og IT gjorde det bra i de fleste sammenhenger, men av disse var det bare offentlig som fikk høy nok signifikans på ANOVA-analysen. Sektoren som gjorde det dårligst på analysen var industri.

Figur 14.a viser et boxplot over spørsmålet om hvor mange som hadde øvelser basert på hendelseshåndteringsplanene. Tallene horisontalt 1(Finans), 2(Helse), 4(Industri), 5(Media), 7(Offentlig), 8(Handel), 9(IT) og 12(Annet), mens tallene 1, 2 og 3 vertikalt står for ja, nei og vet ikke. Som figuren viser så er offentlig sektor klart bedre på øvelser basert på hendelseshåndteringsplanene. Dette bekrefter ANOVA-analysen, med en signifikans på 99,7%. Dette er veldig høyt, og man kan si med veldig stor sannsynlighet at dette stemmer. Figur 14.b viser et boxplot



(a) Boxplot øvelse

(b) Boxplot CaseDu

Figur 14: Figur A viser boxplot over hvor mange som har øvelser innen hendelseshåndtering, mens figur B viser spørsmålet om hvor godt respondenten trodde han/hun ville håndtere en sikkerhetshendelse

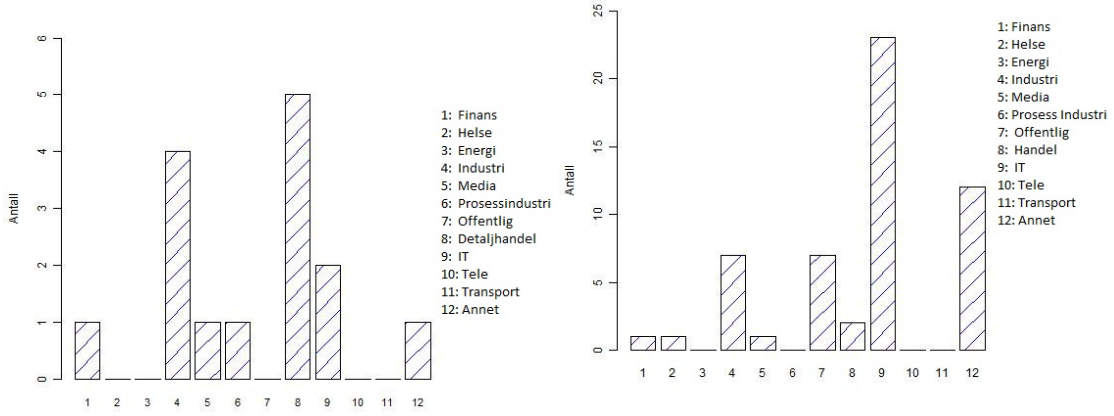
over spørsmålet på hvordan respondenten trodde han ville håndtere en sikkerhetshendelse. Tallene er satt opp på lik måte som i figur A, bortsett fra at tallene vertikalt går fra 1(dårlig) til 5(bra). Figuren viser at industri har mindre tro på seg selv under en sikkerhetshendelse. Dette bekrefter ANOVA-analysen, med en signifikans på 97,8%.

3.2 Dybdeintervju

Dybdeintervju ble valgt som fremgangsmåte for å gå undersøke enda dypere hvordan tilstanden er i norske virksomheter. Det ble her tatt med flere spørsmål, og mer spesifikke spørsmål enn i spørreundersøkelsen. Hensikten med dybdeintervjuene var å samle nok data til å besvare alle hypotesene, samt dybdeinformasjon om håndtering av sikkerhetshendelser i norske virksomheter.

3.2.1 Deskriptiv statistikk

Dybdeintervjuet besto av 52 spørsmål og ble besvart av 15 virksomheter. Spørsmålene ble deretter samlet for å besvare 31 hypoteser som ble satt opp i skjema, som nevnt tidligere i seksjon 2.3.10. Dybdeintervjuet er lagt ved som vedlegg D. I dybdeintervjuet ble det lagt vekt på at det ikke skulle være mange IT virksomheter, ettersom vi hadde mange av disse i spørreundersøkelsen. Spørreundersøkelsen viste at IT og offentlig sektor generelt var flinkere på hendelseshåndtering.



(a) Dybdeintervju sektor

(b) Spørreundersøkelse sektor

Figur 15: Figur A viser virksomheter fra dybdeintervju etter sektor, mens figur B viser virksomheter fra spørreundersøkelse etter sektor

Vi ønsket derfor å samle data fra andre virksomheter for å undersøke om det fantes avvik.

Generelt

Av respondentene så var 54% fra små, 33% fra mellomstore og 13% fra store virksomheter. Som nevnt tidligere i dokumentet 2.3.4, så skulle dybdeintervjuet i hovedsak ta for seg små og mellomstore virksomheter. Vi tok også med to store virksomheter. Grunnen til dette var at vi ønsket å sammenligne store virksomheter mot små og mellomstore, samt undersøke hvordan de arbeidet med hendelseshåndtering.

Som man kan se i figur 15.a så er respondentene fra syv forskjellige sektorer. Sammenligner man med figur 15.b, så ser man at det er ikke tatt med noen virksomheter fra offentlig sektor, og færre fra IT. Grunnen til dette var at boxplot og ANOVA-analysen viste at offentlig og IT var flinkere på mange områder innen hendelseshåndtering. Utvalget for denne undersøkelsen fokuserte derfor på en annen gruppe virksomheter, nemlig handel og industri. Dette fordi ANOVA-analysen av spørreundersøkelsen viste at industri slet mer med hendelseshåndtering. Vi ønsket i tillegg mer handel, ettersom disse var underrepresentert i spørreundersøkelsen, samt at de utgjør en stor del av norske virksomheter, vi mener det derfor ville være interessant å ha med fler av disse. Ettersom utvalget på spørreundersøkelsen og dybdeintervjuet er såpass forskjellige, vil det forekomme avvik i resultatene. Industri og handel er i tillegg preget av virksomheter som driver med mye fysisk arbeid og har strenge krav til HMS. Dette vil også sette preg på undersøkelsen, og mulig gjøre svarene noe bedre, enn den reelle situasjonen i gjennomsnittsvirksomheten.

Sikkerhetsstillinger

Det kan være viktig å ha en sikkerhetsrelatert stilling i virksomheten, en som har ansvar for administrativ sikkerhet som for eksempel utvikling av styringsdokumenter og planlegging. Vi ønsket å undersøke om det fantes en sammenheng mellom det å ha CISO og god hendelseshåndtering. 53% av respondentene svarte at de hadde en som var ansvarlig for informasjonssikkerhet. Enten som egen CISO stilling, eller kombinert med en annen stilling. Vi spurte også om det fantes andre sikkerhetsrelaterte stillinger, 60% av respondentene svarte at de hadde dette. Dette var som oftest stillinger som verneombud og HMS ansvarlig.

Policy

Resultatene fra spørreundersøkelsen viste at de fleste virksomheter hadde informasjonssikkerhetspolicy, mens bare omlag 50% hadde en hendelseshåndteringsplan. I dybdeintervjuene er industri og handelsvirksomheter sterkere representert, mens IT er lavere representert. Et interessant funn er at færre har informasjonssikkerhetspolicy, mens flere har hendelseshåndteringspolicy. Dette kommer nok av som nevnt tidligere, at mange av virksomhetene er påkrevd verneombud og har strenge retningslinjer for HMS.

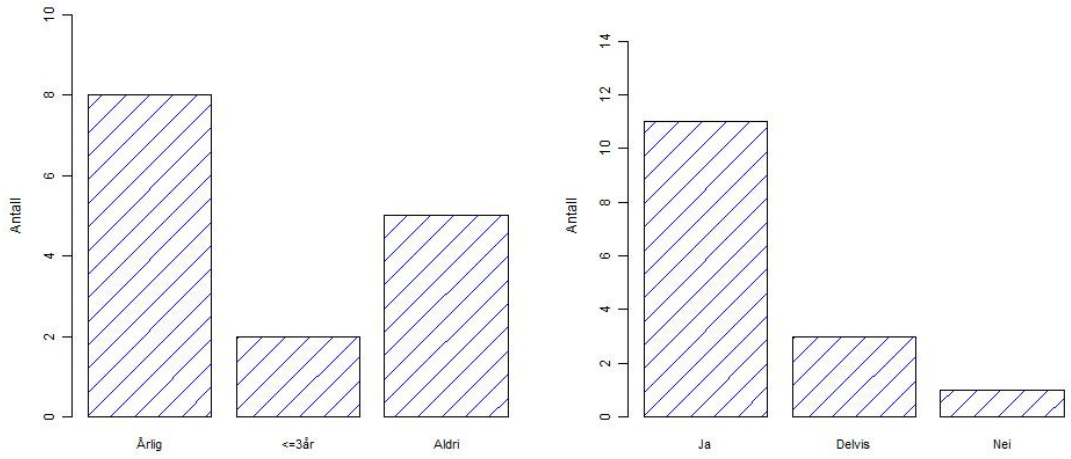
- 47% av virksomhetene hadde ikke noen form for informasjonssikkerhetspolicy.
- 73% hadde helt eller delvis en hendelseshåndteringspolicy.
- 67% hadde helt eller delvis en hendelseshåndteringspolicy som tilstrekkelig.
- 60% hadde en policy som dekket hendelseshåndtering som var underskrevet av en i toppledelsen.

Som figur 16.a viser, så svarte 53% at de reviderte hendelseshåndteringspolicy årlig, 13% svarte at de reviderte hendelseshåndteringspolicy oftere enn hvert tredje år, mens 34% svarte at de ikke hadde revisjon av hendelseshåndteringspolicy i det hele tatt.

Opplæring

Vi undersøkte om virksomhetene hadde opplæringsrutiner innenfor hendelseshåndtering. Hele 93% av virksomhetene mente de hadde dette, enten helt eller delvis. Allikevel så mente bare 40% at opplæringen var tilstrekkelig, 47% svarte delvis, mens 13% mente den ikke var tilstrekkelig. Resultatet er vist i figur 16.b.

Som nevnt under seksjon 3.1.1 om opplæring under spørreundersøkelsen, så er det svakeste



(a) Revisjon av hendelseshåndterings policy

(b) Opplæring innenfor hendelseshåndtering

Figur 16: Figur A viser barplot over revisjon av hendelseshåndteringspolicy, mens figur B viser hvor mange som har opplæring på hendelseshåndtering

leddet oftest mennesket. Det er derfor viktig at alle ansatte får opplæring innen hendelseshåndtering, ettersom det bare kreves en feil for at en sikkerhetshendelse kan intreffe. Vi undersøkte derfor om opplæringen ble repetert for øvrige ansatte, på dette svarte 47% ja, 20% delvis og 33% nei.

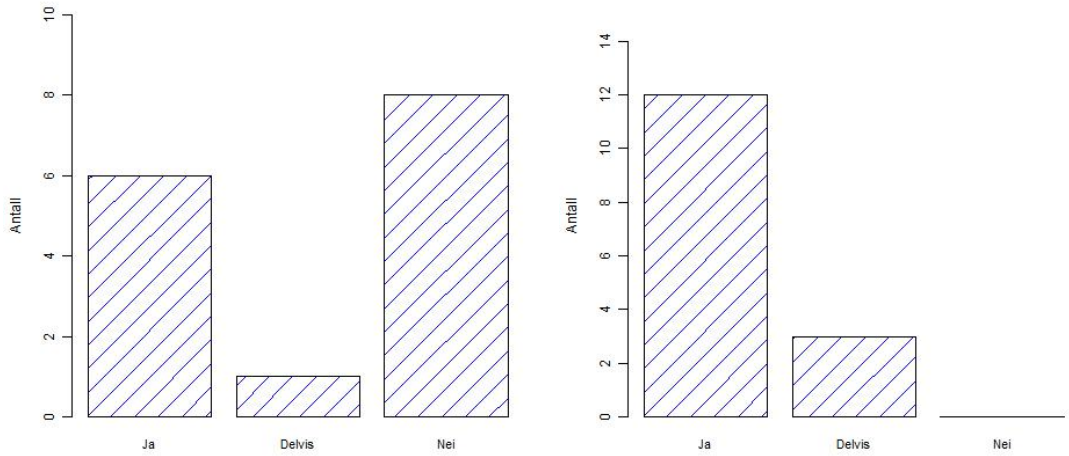
Det er også viktig at opplæringsplaner holdes oppdatert, siden trusselbildet forandrer seg hele tiden. Allikevel svarte 47% at de ikke hadde årlig revisjon av opplæringsplaner.

Hendelseshåndtering

I spørreundersøkelsen undersøkte vi forhold rundt hendelseshåndtering, som f.eks. hvor mange som hadde satt av midler til hendelseshåndtering, og hvor mange som hadde dedikert sikkerhetspersonell som håndterte sikkerhetshendelser. I dybdeintervjuet så fokuserte vi mer på om hendelseshåndteringsplanene inneholdt det en hendelseshåndteringsplan burde inneholde, og hvor mange som hadde disse og fulgte dem.

73% svarte at de helt eller delvis hadde hendelseshåndteringsplaner. Resultatet var det samme når vi spurte om hvor mange som brukte disse under sikkerhetshendelser.

I hendelseshåndteringsplanene så hadde:



(a) Revisjon av hendelseshåndteringsplan

(b) Rapporterer sikkerhetshendelser til ledelsen

Figur 17: Figur A viser oversikt over revisjon av hendelseshåndteringsplan, mens figur B viser oversikt over hvor mange som rapporterer sikkerhetshendelser til ledelsen

- 53% en klart definert trigger.
- 47% klart fordelte ansvarsroller.
- 40% et klart definert omfang.
- 40% planer for revisjon av hendelseshåndteringsplanene. Se figur 17.a.
- 67% klare prosedyrer for varsling.

40% hadde ikke vurdert hvilke verdier virksomheten hadde, eller hvilke trusler den sto opp i mot.

Registrering og rapportering

På spørreundersøkelsen undersøkte vi hvor mange sikkerhetshendelser som ble registrert, og hvor mange som ble rapportert videre til ledelsen. Analysen av spørreundersøkelsen viste at virksomhetene som registerte sikkerhetshendelser også rapporterte disse videre til ledelsen. I dybdeintervjuet så undersøkte vi om det var forskjell på tekniske og ikke-tekniske metoder for registrering av sikkerhetshendelser. Og om virksomhetene foretrakk den ene fremfor den andre.

Vedrørende registrering og rapportering så viste dybdeintervjuene at:

- 87% hadde ikke-tekniske metoder for å registrere sikkerhetshendelser.
- 93% hadde tekniske metoder for å registrere sikkerhetshendelser.
- 40% førte ikke statistikk over sikkerhetshendelser.
- 80% rapporterte sikkerhetshendelser videre til ledelsen 20% mente de gjorde dette delvis. Jfr. figur 17.b.

Oppfølging

For å undersøke hvordan og hvor godt virksomhetene fulgte opp sikkerhetshendelser spurte vi noen spørsmål om oppfølging. Vi undersøkte da om virksomhetene følger opp sikkerhetshendelser, om det fantes konsekvenser dersom ansatte ikke fulgte planene eller retningslinjene, og om virksomhetene hadde noen form for debriefing av ansatte i etterkant av en sikkerhetshendelse.

Resultatet var som følger:

- 93% mente at dersom det oppdages en sikkerhetshendelse, gjorde de også noe med den.
- 60% mente de helt eller delvis hadde konsekvenser dersom de ansatte ikke følger planen/retningslinjene i løpet av en sikkerhetshendelse.
- 80% svarte at de hadde en form for debriefing i etterkant av en sikkerhetshendelse.

Annet

Vi spurte virksomhetene om hva de trodde ville fungere bra og hva som ville fungere dårlig i deres virksomhet under en sikkerhetshendelse. Resultatet er vist i tabell 2.

Tabell 2: Tabell over hva respondentene tror vil fungere bra og dårlig i deres virksomhet.

Vil fungere bra	**Vil fungere dårlig**
Rapporteringen	Forbedring av tiltak etter en sikkerhetshendelse
Samarbeid	Forståelse og kunnskap om IT
Erfaring	Mangel på fagfolk
Kunnskap	Kan ta lang tid
Ansatte	Krisekommunikasjon
Rask responstid	Rapportering av egenskyldte sikkerhetshendelser
Oppfølging	Ansatte utsatt ved ran
Lære av sikkerhetshendelsen	Ansvarsfordeling
God fysisk sikkerhet	Rom for feiltolkning av retningslinjer
Tidlig varsling	

Tabellen 2 viser at enkelte punkter vises under både 'vil fungere bra' og 'vil fungere dårlig'. Det er to tilfeller hvor punktene overlapper. Disse er som følgende: **kunnskap - forståelse og kunnskap om IT**, og **rask responstid - kan ta lang tid**. Vi undersøkte om det her fantes forskjell på sektorene som hadde deltatt på dybdeintervjuene. Ved nærmere undersøkelse viste det seg at det var handel som hadde svart at de kunne ha dårlig forståelse og kunnskap om it, samt at det kunne ta lang tid å håndtere en sikkerhetshendelse. Allikevel hadde også respondenter fra handelssektor svart at kunnskap og responstid vil fungere bra. Vi betrakter derfor disse overlappende punktene som ikke signifikante, men tilfeldige.

3.2.2 Korrelasjonsanalyse

Denne seksjonen beskriver de mest interessante funnene av korrelasjonsanalysen. Korrelasjonene er først listet opp i tabell 3, deretter diskutert. For en oversikt over hele analysen, se vedlegg I.

CISO

Korrelasjonsanalysen viste at det var noen korrelasjoner tilknyttet spørsmålet om virksomheten hadde en sjef for informasjonssikkerhet (CISO). Disse var som følgende:

- Dersom virksomheten har en CISO, så blir også hendelseshåndteringsplanene brukt under sikkerhetshendelser.
- Dersom virksomheten har en CISO, så har hendelseshåndteringsplanene et klart definert omfang.
- Dersom virksomheten har en CISO, har også virksomheten vurdert hvordan sikkerhetshendelsen vil påvirke virksomheten(ROS).

Disse punktene viser at dersom virksomheten har en sjef for informasjonssikkerhet, som arbeider med administrasjon og planlegging. Er sjansene større for at virksomheten har tilstrekkelige planer og at nødvendige administrative tiltak som verdi- og trusselanalyse er utført.

Hendelseshåndteringspolicy

Korrelasjonsanalysen viste at de som hadde hendelseshåndteringspolicy, også mente at denne var tilstrekkelig, og ble tilstrekkelig revidert. Analysen viste også at de som hadde hendelseshåndteringspolicy som var signert av ledelsen, også hadde utført verdi og trusselanalyse. Dette bygger igjen oppunder påstanden ovenfor, som forteller at administrativ involvering fører til bedre planlegging.

Tabell 3: Tabell over viktigste korrelasjoner for dybdeintervjuet.

Spørsmålspar	**Korrelasjon**
'Har virksomheten hendelseshåndteringsplaner?' og 'Blir disse planene brukt under sikkerhetshendelser?'	0.91
'Har virksomheten hendelseshåndteringsplaner?' og 'Beskriver den hvordan underretning skal utføres?'	0.96
'Har virksomheten en policy som dekker hendelseshåndtering?' og 'Er hendelseshåndteringspolicyen tilstrekkelig?'	0.89
'Har virksomheten hendelseshåndteringsplaner?' og 'Har den et klart definert omgang?'	0.89
'Har virksomheten en policy som dekker hendelseshåndtering?' og 'Blir den tilstrekkelig revidert?'	0.88
'Blir disse planene brukt under sikkerhetshendelser?' og 'Beskriver den hvordan underretning skal utføres?'	0.87
'Er opplæringen tilstrekkelig?' og 'Har virksomheten vurdert hvordan sikkerhetshendelsen påvirker virksomheten?'	0.83
'Har virksomheten hendelseshåndteringsplaner?' og 'Er ansvarsroller fordelt?'	0.83
'Når blir planen tatt i bruk, finnes det en "trigger"?' og 'Er ansvarsroller fordelt?'	0.83
'Blir disse planene brukt under sikkerhetshendelser?' og 'Har den et klart definert omgang?'	0.8
'Finnes det metoder for å registrere sikkerhetshendelser?' og 'Samles sikkerhetshendelser i statistikk?'	0.8
'Har virksomheten en CISO?' og 'Har virksomheten vurdert hvordan sikkerhetshendelsen påvirker virksomheten?'	0.78
'Blir disse planene brukt under sikkerhetshendelser?' og 'Når blir planen tatt i bruk, finnes det en "trigger"?'	0.76
'Blir disse planene brukt under sikkerhetshendelser?' og 'Er ansvarsroller fordelt?'	0.74
'Har virksomheten en CISO?' og 'Blir disse planene brukt under sikkerhetshendelser?'	0.73
'Er hendelseshåndteringspolicyen underskrevet av en i toppledelsen?' og 'Har virksomheten vurdert hvordan sikkerhetshendelsen påvirker virksomheten?'	0.73
'Når blir planen tatt i bruk, finnes det en "trigger"?' og 'Beskriver den hvordan underretning skal utføres?'	0.73
'Har virksomheten opplæring på hendelseshåndtering?' og 'Utfører bedriften årlig opplæring og repetisjon for alle ansatte?'	0.72
'Har virksomheten opplæring på hendelseshåndtering?' og 'Er opplæringen tilstrekkelig?'	0.71
'Har virksomheten en CISO?' og 'Har den et klart definert omgang?'	0.7

Opplæring

Analysen viste at de som mente de hadde tilstrekkelig med opplæring, også hadde utført en verdi og trusselvurdering. En grunn til dette kan være at det var en del virksomheter fra sektorer som drev med fysisk arbeid og hadde strenge krav til HMS. Det er derfor viktig for virksomhetene å gjøre trusselvurderinger, samt lære opp de ansatte om riktig bruk av utstyr og sikkerhet.

De som hadde opplæring mente også at opplæringen var tilstrekkelig. Analysen viste også at det ble utført årlig revidering på opplæringsplanene.

Hendelseshåndteringsplan

Analysen viste at det var sterk korrelasjon mellom spørsmålet om de hadde hendelseshåndteringsplaner, og om disse blir brukt under sikkerhetshendelser. Dette viser at de som har planer for hendelseshåndtering, også bruker planene, dersom det skulle oppstå en sikkerhetshendelse. Det fantes i tillegg mange andre korrelasjoner tilknyttet bruk og innhold i hendelseshåndteringsplan. Noen av disse er nevnt i listen under:

- Dersom virksomheten hadde hendelseshåndteringsplaner, hadde de også beskrevet hvordan underretning skulle utføres.
- Dersom virksomheten hadde hendelseshåndteringsplaner, hadde hendelseshåndteringsplanen klart definerte ansvarsroller.
- Dersom virksomheten hadde hendelseshåndteringsplaner, hadde også planen et klart definert omfang.
- De virksomhetene som mente de brukte hendelseshåndteringsplanene under sikkerhetshendelser, hadde og beskrevet hvordan underretning skulle utføres.
- De virksomhetene som mente de brukte hendelseshåndteringsplanene under sikkerhetshendelser, hadde også beskrevet trigger i hendelseshåndteringsplan.

Annet

Analysen viste at de virksomhetene som registrerte sikkerhetshendelser, førte og statistikk over sikkerhetshendelser.

3.3 Diskusjoner

Analysen av spørreundersøkelsen og dybdeintervjuet viste mange interessante funn. Og selv om dataene som ble samlet inn kan benyttes til mange ulike analyser, var hovedfokuset vårt å besvare hypotesene som ble satt opp. I tillegg til dette så utførte vi korrelasjonsanalyse for å finne ut om det fantes lineære sammenhenger mellom spørsmål, og ANOVA-analyse for å sjekke om enkelte størrelser eller sektorer var flinkere på hendelseshåndtering enn andre. Vi vil nå diskutere funnene rundt hvert forskningsspørsmål og forsøke og besvare hypotesene.

3.3.1 Avvik mellom spørreundersøkelse og dybdeintervju

Etter å ha sammenlignet den deskriptive statistikken for spørreundersøkelse og dybdeintervju, ser man at det finnes avvik på noen av spørsmålene. Grunnen til dette er som nevnt tidligere at respondentene er forskjellige og kommer fra andre sektorer. Spørreundersøkelsen hadde mange respondenter fra IT og offentlig sektor, som ifølge boxplot og ANOVA-analysen viste seg å være flinkere på enkelte temaer innen hendelseshåndtering. Dybdeintervjuene derimot var preget av virksomheter i sektorer fra handel og industri. Virksomhetene fra disse sektorene hadde stort fokus på- og strenge krav til fysisk sikring og HMS.

Vi mener allikevel at undersøkelsen gir et godt bilde av situasjonen for SMBer i dag, og at de til sammen dekker alle sektorer og gir et bilde av hvor godt gjennomsnittsvirksomheten driver hendelseshåndtering. De avvikene som inntreffer viser ytterpunktene innenfor valgte tema, og gjør det mulig å se forskjeller på sektorene.

3.3.2 Forskningsspørsmål 1

Forskningsspørsmål nr 1 omhandler virksomhetenes bruk av policy, og ble definert slik: *I hvilken grad har virksomheter en hendelseshåndteringspolicy, eller en hendelseshåndteringspolicy de følger?*

Dybdeintervjuet viste at 47% hadde informasjonssikkerhetspolicy, mens spørreundersøkelsen viste at 68,5% hadde informasjonssikkerhetspolicy. Når det kom til hendelseshåndteringspolicy så var situasjonen omvendt. Spørreundersøkelsen viste at bare 48% hadde en hendelseshåndteringspolicy, mens dybdeintervjuet viste at 53% hadde hendelseshåndteringspolicy. Grunnen til dette har sammenheng med utvalget på undersøkelsene. Dybdeintervjuene ble utført hos mange virksomheter som hadde fysisk arbeid som industri og handel, og mange av disse har strenge krav til HMS og sikkerhet. Det er derfor mer naturlig at disse har hendelseshåndteringspolicy isteden for informasjonssikkerhetspolicy. Dermed har bare omlag halvparten av virksomhetene en hendelseshåndteringspolicy, mens litt over halvparten har informasjonssikkerhetspolicy.

Dybdeintervjuene undersøkte nærmere om virksomhetene hadde en hendelseshåndteringspolicy som var tilstrekkelig. Bare 40% hadde dette. Korrelasjonsanalysene viste at virksomheter

med hendelseshåndteringspolicy var flinkere på opplæring, samt at sikkerhetshendelse oftere er definert dersom man har hendelseshåndteringspolicy. Analysene viste også at dersom hendelseshåndteringspolicyen var underskrevet av en i toppledelsen, så var sjansen større for at det var utført verdi og trusselanalyse. Noe som viser at engasjement fra ledelsen på et tidlig nivå, fører til bedre hendelseshåndtering.

3.3.3 Forskningsspørsmål 2

Forskningsspørsmål nr 2 omhandler virksomhetenes bruk av opplæring, og ble definert slik: *I hvilken grad har virksomheter opplæring på hendelseshåndtering?*

Spørreundersøkelsen viste at hele 57% hadde opplæring på informasjonssikkerhetspolicy. Når det gjaldt hendelseshåndtering, 35% hadde opplæring på hendelseshåndteringspolicy, og 24% opplæring på hendelseshåndteringsplaner. Dybdeintervjuene viste at vesentlig flere hadde opplæring innenfor hendelseshåndtering, denne viste at hele 93% hadde helt eller delvis opplæring på hendelseshåndtering. Dette innebærer da alle former for opplæring som har med hendelseshåndtering å gjøre. Dette bidrar til å gjøre svarprosenten litt høyere. Samtidig som utvalget av de ulike undersøkelsene også påvirker resultatet, siden øving på sikkerhetshendelser er høyt prioritert i virksomheter som har fokus på fysisk sikring og HMS.

Til tross for dette gode resultatet svarte respondentene at bare 40% at opplæringen var tilstrekkelig. Dette viser at mange virksomheter har mangelfull opplæring. I tillegg så hadde bare 47% årlig revisjon av opplæringsplaner. Dette kan føre til at mange har utdaterte opplæringsplaner, som igjen fører til dårligere opplæring.

Opplæring for ledelsen

Korrelasjonsanalysen for spørreundersøkelsen viste at virksomheter som hadde opplæring for ledelsen, var flinkere til å ha øvelser basert på hendelseshåndteringsplaner for ansatte, samt debriefing for ansatte. Øvelser er kjempe viktig for at ansatte skal kunne reagere riktig, og håndtere hendelsen på en god måte. Debriefing er også viktig, og kan gi en rekke fordeler som for eksempel:

- Ansatte kan lære av hendelsen.
- Alle ansatte får lik informasjon, for å unngå rykter.
- Kan være viktig for å avslutte en sikkerhetshendelse, slik at ansatte får ro. Spesielt dersom hendelsen var traumatisk.

Det er interessant å se at sannsynligheten for slike administrative tiltak øker dersom virksomheten har hatt opplæring for ledelsen. Dette viser at opplæring for ledelsen fungerer, og at virksomheter som har en ledelse som fokuserer på hendelseshåndtering, også implementerer bedre rutiner rundt hendelseshåndtering.

3.3.4 Forskningsspørsmål 3

Det ble også undersøkt bruk og innhold i virksomhetenes hendelseshåndteringsplaner. Forskningsspørsmålet for dette temaet er som følger: *I hvilken grad implementerer virksomheter hendelseshåndteringsplaner?*

60% har hendelseshåndteringsplaner, dybdeintervjuet viser at disse også blir brukt under sikkerhetshendelser. Dette viser at de som har planer, også bruker planene. Allikevel burde flere virksomheter ha hendelseshåndteringsplaner, ettersom vi syntes at 60% er for lavt. Dybdeintervjuene undersøkte også om planene oppfylte de kravene som ble satt til en hendelseshåndteringsplan: dvs. at den inneholder en trigger, klart definerte ansvarsroller, omfang, varsling og revidering.

Resultat over virksomhetene som møtte kravene:

- 53% hadde en trigger
- 47% hadde klare ansvarsroller.
- 40% hadde klart omfang.
- 67% rutiner for varsling.
- 40% hadde årlig revisjon av hendelseshåndteringsplan.

Selv om 60% mente de hadde en hendelseshåndteringsplan, så hadde bare 40% en plan som møtte kravene som ble stilt. Dette viser at kun 3/5 har implementert hendelseshåndtering, mens 2/3 av disse har en plan som er god nok.

Korrelasjonsanalysen av spørreundersøkelsen viste at det var gjensidig korrelasjon mellom spørsmålene om hvilke tiltak som ble gjort i etterkant av en hendelse. Tiltakene det ble spurt om var: finne ut om planen fungerte, revisjon av hendelseshåndteringsplan og debriefing av ansatte. Undersøkelsen viste at virksomheter som hadde implementert ett av disse, som oftest hadde alle tre.

3.3.5 Forskningsspørsmål 4

Forskningsspørsmål nr 4 omhandler registrering og rapportering, og er definert som følger: *I hvilken grad har virksomheter rapporteringsmekanismer?*.

Dybdeintervjuene viste at 87% hadde ikke-tekniske metoder for å registrere sikkerhetshendelser, og at 93% hadde tekniske metoder for å registrere sikkerhetshendelser. Dette er forholdsvis høyt, og gir et inntrykk av at de fleste norske virksomheter har gode rutiner for å registrere hendelser. I tillegg viser analysene at registrerte sikkerhetshendelser også blir rapportert videre til ledelsen. Dette er også bra. Allikevel så kan det tyde på at det ikke er gode nok rutiner for registrering, ettersom spørreundersøkelsen viser at omlag 48% mener de bare hadde 5 hendelser eller mindre i løpet av 2009. I tillegg så svarer 39% at de ikke vet hvor mange sikkerhetshendelser som ble registrert i 2009. Det kan derfor virke som om virksomhetene har rutiner for registrering av sikkerhetshendelser, men muligens preget av underrapportering og dårlige system for å holde oversikt over sikkerhetshendelsene.

3.3.6 Forskningspørsmål 5

Det siste forskningsspørsmålet omhandler oppfølging av sikkerhetshendelser. Forskningsspørsmålet er som følger: *I hvilken grad har virksomheter oppfølging av sikkerhetshendelser?*.

93% av virksomhetene mente de helt eller delvis fulgte opp sikkerhetshendelser. Dette resultatet var høyere enn forventet. Ettersom det ble vanskelig for oss å undersøke dette nærmere, blir det problematisk å bevise det motsatte. En grunn til at resultatet er såpass høyt, kan være at virksomhetene har dårlig oversikt over antall hendelser, som nevnt i seksjonen over. En mangelfull oppfatning av antall sikkerhetshendelser vil påvirke oppfatningen av om sikkerhetshendelser følges opp.

3.3.7 Andre interessante funn

Analysene som ble utført på spørreundersøkelsen og dybdeintervjuene resulterte i en rekke interessante funn. Vi tar her en diskusjon på de mest interessante.

Store virksomheter og offentlig sektor flinkest

ANOVA-analysen som ble utført på spørreundersøkelsen viste at i alle tilfeller hvor det fantes signifikante forskjeller, så var store virksomheter og offentlig virksomhet flinkere.

Store virksomheter var flinkere på:

- Informasjonssikkerhetspolicy.
- Definert sikkerhetshendelse.
- Øvelser basert på hendelseshåndteringsplanene.
- Anonym rapportering.

Offentlige virksomheter var flinkere på:

- Informasjonssikkerhetspolicy.
- Hendelseshåndteringspolicy.
- Øvelser basert på hendelseshåndteringsplanene.

Dette er et interessant funn, siden tidligere undersøkelser [23] viste at offentlig virksomhet var dårligere på hendelseshåndtering enn private. Økningen er derfor betydelig, siden offentlig sektor var de som gjorde det best på denne undersøkelsen.

Sikkerhetsstillinger

Vi undersøkte i dybdeintervjuet hvilke sikkerhetsstillinger som fantes. 53% av virksomhetene hadde en som var ansvarlig for informasjonssikkerhet(CISO). Vi ønsket med dette å undersøke om det fantes sammenhenger mellom å ha CISO og god hendelseshåndtering.

Dette stemte til en viss grad, siden korrelasjonsanalysen på dybdeintervjuet viste at virksomheter som har CISO, også:

- oftere bruker hendelseshåndteringsplanene under sikkerhetshendelser.
- har hendelseshåndteringsplaner med et klart definert omfang.
- har vurdert hvordan sikkerhetshendelser påvirker virksomheten (ROS).

Dette viser at det å ha en CISO kan føre til bedre rutiner rundt hendelseshåndtering.

3.4 Konklusjoner

I denne seksjonen vil vi forsøke å trekke konklusjoner på hypotesene som ble satt opp. Strukturen er slik at først presenteres hypotesen, deretter følger argumenter for å bevise eller motvise hypotesen.

Hypotese nr 1

Nesten ingen virksomheter følger hendelseshåndteringspolicy, eller har hendelseshåndteringspolicy som er tilstrekkelig.

Spørreundersøkelsen viste at 48% hadde hendelseshåndteringspolicy, mens dybdeintervjuet viste

at 53% hadde det. Ser man disse under ett, så har omlag halvparten av norske virksomheter hendelseshåndteringspolicy. Dybdeintervjuene viste at bare 40% hadde hendelseshåndteringspolicy som var tilstrekkelig. Dette betyr at 4/5 av de som har hendelseshåndteringspolicy, har en som er tilstrekkelig. Vi mener dog at 40% er en del mer enn *nesten ingen*. **Konklusjonen blir derfor at hypotesen ikke stemmer, men at 40% av norske virksomheter har en hendelseshåndteringspolicy som er av tilstrekkelig kvalitet**.

Hypotese nr 2

De fleste virksomheter har dårlig opplæring på hendelseshåndtering.

Dybdeintervjuene viste at hele 93% hadde opplæring på hendelseshåndtering. Til tross for dette høye resultatet så hadde bare 40% opplæring som var tilstrekkelig. Under halvparten (47%) hadde årlig revisjon av hendelseshåndteringsplaner. Selv om mange har en eller annen form for opplæring innen hendelseshåndtering, så er opplæringen i 3/5 tilfeller mangelfull. **Konklusjonen blir at hypotesen stemmer**.

Hypotese nr 3

De fleste virksomheter har mangelfull eller ingen implementering av hendelseshåndtering.

Dybdeintervjuene viste at 60% hadde hendelseshåndteringsplaner. Når vi undersøkte nærmere om planene møtte våre krav til hva en hendelseshåndteringsplan burde inneholde så var det bare 40% som gjorde dette. Dette betyr at 20% av respondentene hadde hendelseshåndteringsplaner, men mangelfulle planer. 40% hadde ingen planer i det hele tatt. Til sammen så har 60% mangelfull, eller ingen implementering av hendelseshåndtering. **Konklusjonen blir at hypotesen stemmer**.

Hypotese nr 4

Virksomhetene generelt har dårlige rapporteringsmekanismer, noe som fører til dårlig oversikt over antall sikkerhetshendelser.

Dybdeintervjuene viste at virksomhetene var flinke på rapportering og registrering. Hele 87% hadde ikke-tekniske tiltak for å registrere sikkerhetshendelser, mens 93% hadde tekniske. Til tross for dette så viste spørreundersøkelsen at 39% ikke visste hvor mange sikkerhetshendelser som ble registrert i 2009, og 48% mente at det var 5 sikkerhetshendelser eller mindre. Vi tror virksomhetene er preget av underrapportering, og at mange har dårlige rutiner og systemer for å registrere sikkerhetshendelser. Siden så mange virksomheter ikke vet hvor mange sikkerhetshendelser som ble registrert foregående år. **Konklusjonen blir derfor at hypotesen stemmer**.

Hypotese nr 5

Dårlig oppfølging av sikkerhetshendelser er en gjenganger i virksomhetene.

Dybdeintervjuene viste at 93% av virksomhetene fulgte helt eller delvis opp sikkerhetshendelser. Vi tror at virksomhetene er preget av dårlige rapporteringsmekanismer og at virksomhetene er preget av underrapportering. Dette kan påvirke resultatet, ettersom det kan ha forekommet flere sikkerhetshendelser enn det som ble registrert. Vi må allikevel forholde oss til det resultatet vi fikk, ettersom vi ikke har resultater som viser det motsatte, eller undersøkt kvaliteten av oppfølgingen. **Konklusjonen blir derfor at hypotesen ikke stemmer**.

4 Avslutning

I dette kapitlet blir oppgaven, og resultatene av dens mål drøftet. Det blir også rettet kritikk mot punkter vi føler kunne vært utført bedre, eller burde vært gjort annerledes. Videre arbeid blir diskutert og en selvevaluering av prosjektgruppen blir foretatt. Til slutt følger en konklusjon av prosjektet.

4.1 Drøftinger

Ut i fra effektmålene som var satt for prosjektet har vi oppnådd resultater. Veiledningen i hendelseshåndtering håper vi vil gjøre hendelseshåndtering lett tilgjengelig for SMBer, dette vil og hjelpe oppdragsgiver å få større fokus rundt hendelseshåndtering. At veiledningen publiseres på oppdragsgivers egne hjemmesider vil bidra til dette. Spørreundersøkelsen og dybdeintervjuene som ble utført bidro forhåpentligvis også til større fokus rundt hendelseshåndtering for de som deltok på disse. I etterkant av spørreundersøkelsen og dybdeintervjuene så vi at vi burde lagt til et spørsmål i spørreundersøkelsen, hvor vi spurte om respondentene var villige til å være med videre i et dybdeintervju. Dette fordi det viste seg å være svært vanskelig å få SMBer til å sette av tid til et slikt intervju.

Rapporten dokumenterer resultatene av spørreundersøkelsen og dybdeintervjuene som ble utført. Innholdet består av funnene som ble gjort, og det har blitt lagt vekt på å besvare forskningsspørsmålene. Med resultatene fra spørreundersøkelsen og dybdeintervjuene har vi fått en bredere oversikt over hvordan SMBer håndterer forskjellige typer sikkerhetshendelser. Rapporten inneholder en statistisk oversikt over resultatene fra undersøkelsene og intervjuene, og diskusjoner og drøftinger av disse. Det har også blitt avdekket relevante aspekter ved hendelseshåndtering.

Etter ønske fra oppdragsgiver har det blitt automatisert statistisk analyse fra spørreundersøkelsen, slik at samme undersøkelsen kan kjøres i fremtiden av oppdragsgiver for å se etter bedring i hendelseshåndteringsarbeid.

De som tar i bruk veiledningen vil få en økt forståelse rundt temaene hendelseshåndtering og IT-sikkerhet. Prosjektgruppen kunne tenkt seg å hatt med mer informasjon i veiledningen, men dette hadde gått på beskostning av veiledningens lengde og leselighet. Mye informasjon ble derfor utelatt fra dokumentet og heller lenket til eksterne websider med utfyllende informasjon. Men vi mener den ble målrettet og holdt jevn fokus hele veien på minimumstiltak som må gjøres.

Det kunne vært arbeidet litt mer med designet på veiledningen, men dette er ikke prosjektgruppens sterkeste fagfelt, det var ikke satt noen krav til designet 2.4.3. Vi gikk derfor for et enkelt og ryddig design.

Det var opprinnelig ment at vi skulle lage to forskjellige veiledninger, en for små virksomheter og en for mellomstore, men dette gikk vi bort fra etter å ha arbeidet med teorien rundt hendelseshåndtering. Begge veiledningene hadde blitt svært like, vi valgte derfor bare å lage én enkel veiledning med minimumskrav. For å gi tilgang til mer utfyllende informasjon om emnene, valgt vi å lenke til utfyllende informasjon i slutten av hvert kapittel. Denne løsningen mener vi var bedre enn å utvikle to separate veiledninger.

Angående implementering av deteksjonsverktøy og rapporteringsmekanismer valgte vi å bruke et kapittel i veiledningen på akkurat dette.

4.2 Kritikk av oppgaven

Det ble overvekt av respondenter fra IT-bedrifter som svarte på spørreundersøkelsen. Vi så ut i fra spørreundersøkelsen at IT-bedrifter er flinke på hendelseshåndtering, så dette kan ha gitt utslag på det totale resultatet.

Kontaktlisten vår kom fra oppdragsgiver. Hvis bedrifter har kontakt med oppdragsgiver er det stor sjanse for at de allerede har fokus på informasjonssikkerhet. Dette kan også ha gitt utslag på resultatet i undersøkelsen. Dette var ikke noe problem i dybdeintervjuene, da hovedgruppen av virksomhetene ikke stammet fra kontaktnettverket til oppdragsgiver.

Det ferdige skriptet og analysene fungerer kun dersom oppdragsgiver kjører den samme spørreundersøkelsen.

Forskningsspørsmål og hypotese nr 1 inneholdt to spørsmål. Disse burde vært delt opp og besvart hver for seg. I tillegg var dette forskningsspørsmålet for uspesifisert, slik at det ble vanskelig å gi en god konklusjon. Ettersom forskningsspørsmålene danner grunnlaget for hele dokumentet, valgte vi å ikke endre dette.

4.3 Videre arbeid

Programmet for vasking av data, skriptet og spørreundersøkelsen er lagt ved i rapporten. Disse kan brukes på nytt i fremtiden til å samle inn nye statistiske data til sammenligning med resultatene i denne rapporten. Oppdragsgiver har da mulighet til å utføre denne undersøkelsen i kommende år, og på denne måten kan de undersøke trender i hendelseshåndtering. De kan da se hvordan norske SMBer anvender hendelseshåndtering fra år til år. Dette kan danne et viktig

grunnlag sammen med mørketallsundersøkelsene [24, 25], for å kartlegge informasjonssikkerheten i norske virksomheter.

Det kan og være nyttig å utføre nye analyser som sammenligner undersøkelsene for hvert år. På denne måten kan man enklere se utviklingen og resultat av iverksatte tiltak.

Vi hadde også planer om å legge veiledningen i en e-læringsmodul, i en ny form for opplæring som kalles nanolearning [27]. Dette fikk vi dessverre ikke tid til. Dette kunne være et lurt steg for å gjøre veiledningen mer attraktiv for SMBer som ønsker å ta den i bruk.

Etter å ha arbeidet med oppgaven ser vi at det er mange temaer som enda ikke er undersøkt, eller kunne vært gjort bedre. Det kunne blant annet vært gjort en større undersøkelse, hvor en har flere respondenter, og nok respondenter fra alle sektorer til å utføre ANOVA-analyse for å finne forskjeller mellom alle sektorene. Det kunne også vært interessant å utføre en undersøkelse, hvor en undersøkte om det fantes forskjeller på hvordan hendelseshåndtering anvendes i de ulike landsdelene i Norge. I tillegg til dette kunne det vært interessant å undersøke på tvers av landene, f.eks. sammenligne Norge opp mot andre nordiske land, eller andre land som har gjort lignende undersøkelser.

Vi undersøkte heller ikke om respondentene anvendte standarder i sin bruk av hendelseshåndtering. Det kunne vært interessant å undersøke om det finnes forskjeller på de virksomhetene som forholder seg til standarder, og andre virksomheter. Det kan også undersøkes hvilke standarder som blir brukt, og hvordan dette resulterer.

Vi fikk ikke tid til å utvikle en mal for hendelseshåndteringspolicy. Dette er noe det er behov for, dersom virksomhetene skal implementere hendelseshåndtering. I tillegg burde det vært utviklet gode eksempler på hendelseshåndteringspolicy og hendelseshåndteringsplaner som kunne vært lagt med veiledningen, slik at virksomhetene har noe å forholde seg til når de skal utvikle policy og planer.

Det kunne også vært interessant å intervjue flere respondenter på dybdeintervjuet, slik at vi fikk en bredere og større respondentbase. Dette ville gitt oss muligheter til en større statistisk analyse og gi større sikkerhet i resultatet.

4.4 Evaluering av prosjektgruppas arbeid

Gruppen har fungert svært godt, og alle har gjort arbeidet som har blitt tildelt dem. Medlemmene i prosjektgruppen har tidligere arbeidet i fellesskap, og går godt sammen. Det har ikke vært noen konflikter, og problemer har blitt løst i fellesskap. Prosjektgruppen har stort sett vært tilstede på HiG fire til fem dager i uka hver uke siden prosjektet startet, noen flere mot slutten av prosjektet. Kommunikasjon mellom gruppemedlemmene har ikke vært noe problem. Det har heller ikke

vært noe alvorlig sykdom som har resultert i fravær i løpet av prosjektperioden.

Rollene i gruppen har vært godt fordelt. Samarbeidet har fungert godt, og det har vært svært få situasjoner der leder har måttet ta styring. Websiden brukte vi til å markedsføre spørreundersøkelsen, og den ble derfor prioritert i begynnelsen av prosjektet. Men oppdateringer av den ble ikke prioritert etter spørreundersøkelsen var avsluttet.

Arbeidsfordelingen innad i gruppen var jevn, men vi ser i ettertid at det statistiske arbeidet burde vært prioritert foran utvikling av veiledningen. Etter spørreundersøkelsen var avsluttet delte gruppen seg. To medlemmer tok fatt på det som sto igjen av utvikling på dybdeintervju og begynte arbeidet med å få tak i intervjuobjekter, mens siste mann tok fatt på det statistiske arbeidet. Gruppen ser i etterkant at det burde vært prioritert annerledes. Gruppen burde prioritert det statistiske arbeidet med to medlemmer og utvikling av veiledningen med ett medlem. Til tross for dette, ble både veiledningen og det statistiske arbeidet ferdig i god tid.

Prosjektgruppen har tidligere arbeidet sammen på store prosjekter, så dette var verken noe nytt eller noe problem. Dette var derimot en positiv faktor i prosjektet. Grunnen til dette, var at gruppens medlemmer kjente hverandres styrker og svakheter, dette førte til at arbeidet ble utført raskt og effektivt. Utviklingen av prosjektrapporten ble startet tidlig og har vært en kontinuerlig prosess der alle gruppemedlemmene har bidratt mye.

Oppdragsgiver har vært svært hjelpsom, vi har hatt møte med veileder og oppdragsgiver en gang annenhver uke, der vi har fått tilbakemelding på arbeid og kommentarer på ting vi burde gjøre. En av prosjektgruppas medlemmer er deltidsansatt hos oppdragsgiver, dette har ført til at vi har hatt veldig god kommunikasjon. Gruppas veileder har også bidratt svært mye i prosjektet og hjulpet oss når vi har trengt det.

Arbeidsmengden har vært jevnt fordelt utover hele perioden, vi har overholdt tidsfrister satt i Gantt-skjemaet. Den første store milepælen var å få ut spørreundersøkelsen. Vi arbeidet hardt med å få utviklet og lansert den i god tid. Dette gikk fint og den var allerede avsluttet i slutten av februar. Vi klarte også å bli ferdige med de fleste dybdeintervjuene til påske, noe som vi også hadde tidspress på.

Veiledningen var det eneste som ble forsinket, men dette ordnet vi ved at bare ett prosjektmedlem jobbet med å gjøre den ferdig, mens de to andre medlemmene jobbet fulltid på rapporten. Bortsett fra dette har arbeidet gått fint, det har selvsagt vært litt mer jobb mot slutten av prosjektet, men vi har jobbet jevnt over hele prosjektperioden, så det har ikke blitt noen store stressperioder.

4.5 Konklusjon

Vi er svært fornøyde med å ha gjennomført bacheloroppgaven vi valgte. Det har vært en svært spennende prosess der vi har lært mye nytt. Å gjennomføre et prosjekt som er av betydning for en ekstern oppdragsgiver har vært svært givende. Og det å vite at det vi leverer blir brukt hvis det var av forventet kvalitet, har vært en ekstra motivasjon for å gjøre oppgaven bra.

Vi har ikke fått brukt så mye av de tekniske ferdighetene vi har lært i løpet av våre 3 år på HiG, siden vi valgte en oppgave som ikke hadde behov for mange tekniske løsninger (bortsett fra et vaskeprogram og et skript). For å løse prosjektoppgaven har vi hatt spesielt god nytte av det vi lærte i faget Sikkerhetsplanlegging og hendelseshåndtering. Vi har også benyttet oss av tilegnet kunnskap fra fagene Systemutvikling, Risikostyring og Sikkerhet i datasystemer.

I løpet av prosjektet har vi lært svært mye om teorien rundt hendelseshåndtering, vi har også hatt det privilegium å få intervjue virksomheter som bruker dette i praksis. Det å få se hvordan norske virksomheter prioriterer når de skal implementere sikkerhet har vært svært lærerikt.

Den overordnede konklusjonen på prosjektet vårt er at vi fikk svart tilstrekkelig på alle forskningsspørsmålene, slik at vi kunne konkludere med et solid svar på alle hypotesene. Undersøkelsene viste at om lag halvparten av virksomhetene hadde hendelseshåndteringspolicy, av disse hadde 4 av 5 policyer som opprettholdt tilfredsstillende kvalitet. De fleste virksomhetene hadde dårlig opplæring på hendelseshåndtering. Selv om resultatene viste at ca 90% hadde en form for opplæring, viste resultatene at kun 40% av virksomhetene hadde opplæring som var av tilstrekkelig kvalitet. Når det gjaldt implementasjon av hendelseshåndtering, hadde de fleste mangelfull eller ingen implementasjon. Resultatene fra undersøkelsene viste at 60% av alle virksomhetene enten hadde for dårlige planer, eller ingen planer i det hele tatt. Undersøkelsene viste også at virksomhetene hadde dårlige rapporteringsmekanismer, noe som kan føre til dårlig oversikt over antall sikkerhetshendelser. Til tross for dette, viste undersøkelsen at virksomhetene hadde god oppfølging av sikkerhetshendelser, men resultatene på hypotesen om rapportering har ga mistanker om at underrapportering har vært en stor faktor for det positive resultatet i denne konklusjonen.

Korrelasjonsanalysen viste også interessante funn, som for eksempel at opplæring for ledelsen fungerer. Virksomheter som hadde opplæring for ledelsen var flinkere til å gjennomføre øvelser for ansatte, samt ha debriefing for ansatte i etterkant av en sikkerhetshendelse. Det kom også frem at det fantes klare fordeler ved å ha en CISO. Virksomheter med CISO anvender oftere hendelseshåndteringsplanene under sikkerhetshendelser og har bedre hendelseshåndteringsplaner. Det viste seg også at virksomheter med CISO i større grad hadde utført verdi- og trusselvurdering.

ANOVA-analysen viste at det fantes forskjell på norske SMBer. Den viste at offentlig sektor var flinkere enn privat sektor på mange områder innen hendelseshåndtering. Det samme gjaldt store virksomheter, disse skilte seg positivt ut i mange sammenhenger.

Vi er svært fornøyde med resultatet, og glade for å kunne bidra med ny kunnskap om hvordan norske SMBer anvender hendelseshåndtering. Vi er også fornøyde med resultatet på veiledningen og håper den vil hjelpe SMBer til å utvikle gode hendelseshåndteringsplaner i fremtiden.

Bibliografi

[1] Finansdepartementet. Små og mellomstore bedrifter. http://www.regjeringen.no/nb/dep/fin/dok/nouer/1995/nou-1995-16/5/2/1.html?id=336716.

[2] Guttu, T. 2004. *Norsk Ordbok*. Kunnskapsforlaget.

[3] Gunnar G, L. 2004. *Statistikk for Universiteter og Høgskoler*. Universitetsforlaget.

[4] Norsk senter for informasjonssikring. http://www.norsis.no.

[5] Internet world stats. http://www.internetworldstats.com/europa2.htm#no.

[6] Statistisk sentral byrå.

[7] for Standardization, I. O. 2004. Iso 18044.

[8] Swanson, m. f. 2002. Nist 800-34.

[9] Mattord, W. . 2007. *Incident Respons and Disaster Recovery*. Thomson, course techonoly.

[10] Andreas Gulliksen, a. N. Questback, ask & act. http://www.questback.com.

[11] latex project.org. Latex - a document preparation system. http://www.latex-project.org/.

[12] Schneider, D. K. Theory driven research designs. http://tecfa.unige.ch/guides/methodo/edu-tech/slides/res-design-quant.pdf.

[13] van Exel, J. Qmethodology. http://www.qmethodology.com.

[14] How to effectively write a tutorial. http://richworks.in/2010/03/how-to-effectively-write-a-tutorial/.

[15] Socco, D. 11 essential tips to writing the ultimate tutorial. http://www.dailyblogtips.com/11-essential-tips-to-writing-the-ultimate-tutorial/.

[16] for Standardization, I. O. 2008. Iso 9001.

[17] The r project for statistical computing. http://www.r-project.org/.

[18] i Oslo, U. Universitetet i oslo - deskriptiv statistikk. http://www.bio.uio.no/plfys/haa/littav/stat.htm#deskriptiv.

[19] TimeWeb. Timeweb - forklaring på korrelasjon. http://www.bized.co.uk/timeweb/crunching/crunch_relate_expl.htm.

[20] Microsoft excel. http://office.microsoft.com/excel.

[21] Spss. http://www.spss.com/.

[22] Gcc, the gnu compiler collection. http://gcc.gnu.org/.

[23] Orderløkken, T. L. 2005. Security incident handling and reporting, a study of the difference between theory and practice.

[24] 2003. Mørketallsundersøkelsen fra 2003 utarbeidet i samarbeid av økokrim, næringslivetssikkerhetsråd og norsk senter for informasjonssikring. http://www.nsr-org.no/docs/79281401M.pdf.

[25] 2008. Mørketallsundersøkelsen fra 2008 utarbeidet i samarbeid av næringslivetssikkerhetsråd, statoilhydro, norsk senter for informasjonssikring, kripos, nasjonalsikkerhetsmyndighet, sintef og secode. http://www.nsr-org.no/materiell.htm.

[26] sikkerhetsmyndighet, N. Nsm nettsamfunn og sikkerhet. https://www.nsm.stat.no/Documents/Temahefter/2008_0506_Nettsamfunn&Sikkerhet_NSM_web.pdf.

[27] Junglemap. Nanolearning. http://www.junglemap.com/.

A Vedlegg: Veiledning i Hendelseshåndtering

Veiledning i hendelseshåndtering

Håndtering av sikkerhetshendelser for små og mellomstore bedrifter

Introduksjon

Denne veiledningen er utviklet for små og mellomstore virksomheter. Veiledningen tar for seg hvorfor og hvordan man planlegger håndtering av sikkerhetshendelser, hvordan man utfører en verdivurdering og generelt om de forskjellige typene tiltak man bør gjøre for å skape bedre sikkerhet rundt virksomheten.

Veiledningen forutsetter at man har det grunnleggende sikkerhetsarbeidet på plass. Dersom virksomheten tidligere ikke har utført noen form for sikkerhetsarbeid anbefaler vi å besøke NorSIS sine veiledningssider. De finner du her [4].

Etter å ha utført tiltakene beskrevet i denne veiledningen vil du sitte igjen med:

- En solid hendelseshåndteringspolicy.
- Gode planer for håndering av sikkerhetshendelser som er aktuelle for din virksomhet.
- Generelt bedre sikkerhet.

Definere og identifisere en sikkerhetshendelse

Med sikkerhetshendelse mener vi et avvik som kan ha konsekvenser for virksomhetens daglige drift. Håndtering av sikkerhetshendelser omhandler sikkerhetshendelser av ikke alvorlig grad som kan true virksomheten. Vi vil ikke ta for oss katastrofehåndtering i denne veiledningen.

Det eksisterer flere kategorier sikkerhetshendelser, noen er forårsaket av mennesker, andre kan være naturskapt. For en IT-bedrift kan en type sikkerhetshendelse være virusangrep, virusangrep kan forekomme hyppig og kan få alvorlige konsekvenser for virksomheten hvis ansatte handler feil. For byggebransjen kan en sikkerhetshendelse være definert som en ulykke hvor ansatte pådrar seg personskader. Alvorlige sikkerhetshendelser for en virksomhet som driver handel kan være innbrudd og brann.

Det er viktig at alle ansatte i bedriften er inneforstått med hva en sikkerhetshendelse er, hvis de ikke vet hva det er, kan de heller ikke rapportere det. Det bør også være klart hvem de ansatte rapporterer til, og at det blir igangsatt tiltak når sikkerhetshendelsen rapporteres.

Hvorfor hendelseshåndtering?

"*By failing to prepare, you are preparing to fail*" – Benjamin Franklin

Det første en spør seg er kanskje hvordan og hvorfor man skal forholde seg til hendelseshåndtering, og sikkerhet generelt. Gjengitt fra ROSI [13] (Return On Security Investment) modellen har man følgende spørsmål en bør stille seg selv før man går løs på sikkerhetsarbeidet: Hvor mye koster det virksomheten å ikke håndtere sikkerhetshendelser? Hvor stor innvirkning har det på produktiviteten? Hvilke løsninger er de mest kostnadseffektive? Hvilken innvirkning vil disse løsningene ha på produktiviteten? Sikkerhetshendelser oppstår hos alle virksomheter, enten de er tekniske, fysiske eller logiske. I en eller annen form vil virksomheten få bruk for hendelseshåndtering. En av de større utfordringene ligger i det å kunne detektere sikkerhetshendelser, og det å gjøre dette på en kostnadseffektiv måte.

Undersøkelsen viser at 33 % av norske virksomheter ble utsatt for datakriminalitet i løpet av 2007.
- Hentet fra mørketallsundersøkelsen 2008

Hvordan man håndterer, eller ikke håndterer en sikkerhetshendelse kan påvirke omdømmet til virksomheten din. Med skadet omdømme risikerer man nedgang i fortjeneste. En skal heller ikke glemme at man har ansvar for informasjonen man er i besittelse av. Havner sensitive personopplysninger på avveie vil det være ditt ansvar. Det er lovpålagt [7] (**§ 9.** *Behandling av sensitive personopplysninger* , **§ 13.** *Informasjonssikkerhet*) sikring på denne typen informasjon, dersom noe slikt skulle inntreffe vil det være din virksomhet som må svare for seg, både til rettsvesenet og til media/offentligheten.

Ved hjelp av denne veiledningen skal du kunne utvikle planer og gjøre tiltak som sørger for at du og din virksomhet står best mulig rustet og forberedt til å kunne håndtere sikkerhetshendelser som oppstår.

Når må en sikkerhetshendelse håndteres?

Sikkerhetshendelser må håndteres når de er av en slik alvorlighetsgrad at det går utover virksomhetens daglige drift. Det blir oppdaget innbrudd i din virksomhets lokaler, innbruddstyvene får med seg flere datamaskiner, her må det kartlegges hva som gikk tapt. Hvilke data har blitt stjålet? Hvem har ansvaret? Hvem skal kontaktes og i hvilken rekkefølge? Hvordan opprettes tapte data? Når er virksomheten ferdig med sikkerhetshendelsen? Slike spørsmål vil en god hendelseshåndteringsplan gi klare svar på, gode planer vil hjelpe virksomheten håndtere sikkerhetshendelsen og sørge for at de er tilbake til normal drift raskt og effektivt.

1. Utvikle hendelseshåndteringspolicy

En hendelseshåndteringspolicy er et overordnet styringsdokument som skal ligge til grunn for utvikling av alle hendelseshåndteringsplaner. Den skal også beskrive målsetninger som bedriften setter seg innenfor hendelseshåndtering. Gode hendelseshåndteringsplaner har alltid en god hendelseshåndteringspolicy å støtte seg på.

(Setninger og punkter merket i tykk skrift er minimumskrav, uavhengig av bransje eller størrelse på virksomhet)

Policyen bør inneholde:

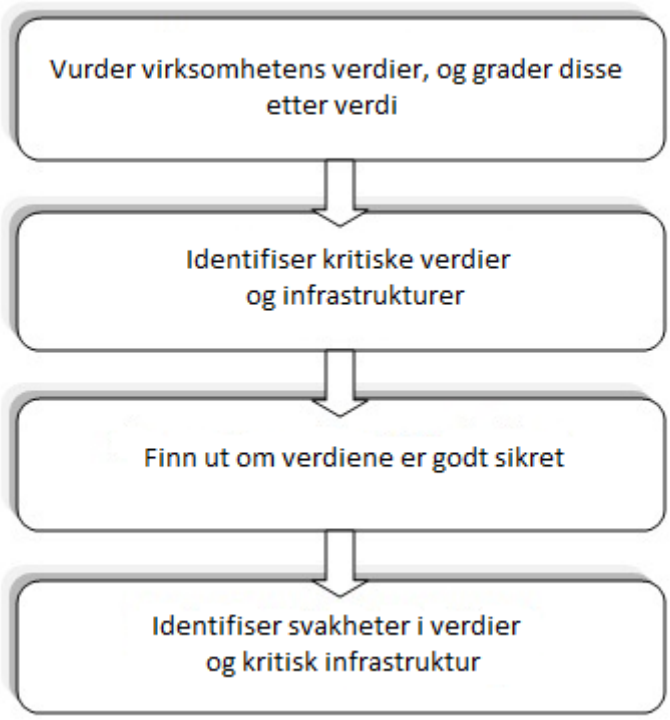
- **Et utsagn fra ledelsen som sier hvor viktig hendelseshåndtering er for virksomheten i sin helhet.**
- **Klart definert omfang, rammer og meningen med hendelseshåndteringspolicyen.**
- **Krav for å utføre risikovurderinger og verdivurdering (Business Impact Analysis) etter behov eller årlig.**
- **Beskrive viktige lover, standarder og reguleringer som må/bør tas til føle, og deres relevans.**
- **Fordele roller og ansvar innad i organisasjonen under hendelseshåndterings-operasjoner.**
- **Krav om at planene testes regelmessig.**
- **Krav til opplæring.**
- En appell til alle virksomhetens ansatte om å gi sin støtte til planen for å involvere dem i den.
- Ekstra administrativ informasjon som inkluderer dato policyen ble gitt ut, revisjoner, orginal forfatter, og et skjema for periodisk oppdatering og vedlikehold av policyen.

  For mer informasjon rundt utvikling av hendelseshåndteringpolicy, les NIST 800-34 [9] eller Principles of Incident Response and Disaster Recovery [3].

2. Verdi og trusselvurdering (Business Impact Analysis)

Hensikten med å utføre en verdi og trusselvurdering (BIA – Business Impact Analysis) av virksomhetens verdier er å identifisere de viktigste eiendelene, hvilke trusler disse står overfor og hvilke av de som må beskyttes. BIA handler om å forstå hva som er kritisk for virksomheten, og hvilke konsekvenser (økonomiske og andre) det får for virksomheten hvis tjenesten / eiendelen blir utsatt for en sikkerhetshendelse. BIA kan også ses på som en analyse av hva man bør beskytte og hva man har råd til å la være å beskytte.

På bakgrunn av vurderingen vil virksomheten bedre kunne forutsi hva de bør gjøre i forkant for å sikre mot og begrense effekten av en sikkerhetshendelse.



Figur 1: Fremgangsmåte for verdivurdering

For en mer utdypende informasjon om hvordan en utfører Business Impact Analysis anbefales det å lese NIST sp800-34 [9] og NSM sin veiledning på verdivurdering [5].

Risikovurdering er en del av verdivurderingen, vi har tatt utgangspunkt at virksomheten har utført en risikovurdering før det arbeides med denne veiledningen. Dersom virksomheten mangler en risikovurdering, eller det ønskes mer informasjon om dette anbefales det å lese NorSIS veiledning for risikostyring [4].

3. Forebyggende tiltak

"*Security is always excessive until it's not enough*." — Robbie Sinclair, Head of Security, Country Energy, NSW Australia

En av de mer kostnadseffektive måtene å håndtere sikkerhetshendelser er å håndtere de før de oppstår. Her er det listet opp noen tiltak som en bør vurdere å implementere.

(Setninger og punkter merket i tykk skrift er minimumskrav, uavhengig av bransje eller størrelse på virksomhet)

Tekniske tiltak

- **Antivirusprogram (f.eks: Norton, Norman, Macaffe, AVG), og loggløsninger på de forskjellige klientene.**
- **Brannmur, vil kunne blokkere og filtrere bort en rekke angrep.**
- **Backup**
- Kryptering av data og trådløse nettverk

Fysiske tiltak

- **Alarmsystemer (innbruddsalarm, brannalarm)**
- **Rapporteringsystemer for de ansatte (telefon, mail)**
- **Låser/fysisk sikring**

Management

- **Jevnlige analyser på trusselbildet**
- Opplyse de ansatte om trusselbildet

De tekniske tiltakene; brannmur og antivirusprogram, er minimumstiltak.
Dette er veldig enkle og rimelige tiltak. Uten en brannmur og antivirusprogram hvordan skal du da oppdage angrep? Disse alene kan være nok til å redusere antall sikkerhetshendelser mot virksomheten. Etter endt sikkerhetshendelse bør man undersøke ut om det er mulig å gjennomføre forebyggende tiltak for å forhindre en gjentagelse av den spesifikke sikkerhetshendelsen.

For mer informasjon angående sikkerhetskopiering/backup anbefales det å lese NorSIS sin veiledning. Den finner du her [4].

4. Utvikle gjenopprettingsstrategier

Etter endt sikkerhetshendelse bør målet være å få virksomheten raskt tilbake til normal drift. Nedetid er tapte inntekter. For å gjøre dette effektivt er det nødvendig å ha en gjenopprettingsstrategi.

Det eksisterer flere typer tiltak man kan gjøre for å kunne foreta en gjenoppretting. Dette kan innebære backup av data, relokalisering, eller nødsystemer som strømaggregater.

(Setninger og punkter merket i tykk skrift er minimumskrav, uavhengig av bransje eller størrelse på virksomhet)

Hva du bør vurdere i din plan:

- **Hvilke rutiner skal være på plass for hvordan du skal gjennomføre backup.**
- **Hvilke backup løsninger du skal ha(f.eks Full redundans).**
- **Hvor ofte man gjennomfører backup, og hva man tar backup av.**
- Hvilke rutiner skal være på plass for hvordan du skal gjennomføre gjenoppretting.
- Finnes det klare ansvarsroller for hvem som skal utføre backup og gjennoppretning.
- Nødvendigheten av å ha backup på forskjellige lokasjoner
- Få dette ned på papir, og sørg for at de ansatte er underrettet om rutiner.

For mer informasjon angående sikkerhetskopiering/backup anbefales det å lese NorSIS sin veiledning. Den finner du her [4].

Når det gjelder avhengighet og bruk av IKT vil 2 av 3 virksomheter få store problemer dersom sentrale IT-systemer er ute av drift i mer enn 1 dag.
- Hentet fra mørketallsundersøkelsen 2008

5. Utvikle en hendelseshåndteringsplan

Utifra vurderinger gjort under BIA lages det en hendelseshåndteringsplan per scenario, som virksomheten finner sannsynlig at kan forekomme. Denne planen skal dekke hele scenarioet fra begynnelse til slutt.

Lag en individuell plan for hvert scenario som ble vurdert så alvorlig at det må håndteres. Under er det en plan som inneholder minimumskravene, og er et godt utgangspunkt for en hendelseshåndteringsplan.

Hendelsestype:	
Trigger:	
Ansvarsroller og leder:	
Kommunikasjon under hendelsen:	
Varsling:	
Responstid:	
Håndtering av hendelsen steg for steg:	
1	
..	
n.	
Hendelsen er over når:	
Handlinger som skal utføres når hendelsen er over:	
1	
..	
n.	
Oppfølging av hendelsen og handlinger i etterkant er avsluttet når:	

Figur 2: Eksempel på hendelseshåndteringsplan. (Oversatt fra Whitman og Mattords "Incident Response and Disaster Recovery"[3])

Her er det listet opp hva en god hendelseshåndteringsplan må inneholde.

1. Omfang:
I eksempelet over blir omfang definert som hendelsestype. Omfanget bør definere hvilken type angrep eller sikkerhetshendelse det er snakk om.

2. Trigger/utløser:
En trigger/utløser definerer når en plan skal tas i bruk. En trigger/utløser fungerer som et klart signal på at planen skal tas i bruk. Dette kan f.eks være:

- En e-post fra systemadministrator om uvanlig trafikk på det interne nettverket.
- Intrusion detection systemer som sier ifra om innbrudd på nettverket.
- Brannalarm, og/eller eventuelle andre type alarmer.

3. Ansvar og roller:
Ansvar og roller defineres i dokumentet. Ansatte har forskjellige ferdigheter, derfor kan ansvar og roller være avhengig av hvilken type sikkertshendelse det er. Fysisk inbrudd og et nettverksinnbrudd er gode eksempler på sikkerhetshendelser som krever forskjellige typer ferdigheter.

Rollene som blir beskrevet her skal gjelde fra sikkerhetshendelsen oppstår til den er avsluttet. (I eksempelet er det definert som ansvarsroller og leder)

4. Kommunikasjon:
Beskriver hvordan kommunikasjon skal foregå mellom de involverte i hendelseshåndteringen og hvilke kommunikasjonsmidler som skal brukes. En virksomhet kan for eksempel ha

walkietalkier eller telefoner dedikert til kommunikasjon under sikkerhetshendelser.

5. Varsling:
Beskriver hvordan de involverte i sikkerhetshendelsen og hendelseshåndteringen skal varsles.F.eks telefonlister.

6. Krav til responstid:
Responstid er tiden det tar virksomheten fra de oppdager sikkerhetshendelsen, til de er klare til å håndtere den.

7. Håndtering av sikkerhetshendelsen:
Dette punktet beskriver trinnvis hva som skal gjøres for å håndtere sikkerhetshendelsen, mens den pågår. Punktet inneholder stegene for å håndtere sikkerhetshendelsen. Dette vil være den mest omfattende delen av hendelseshåndteringsplanen.

8. Når sikkerhetshendelsen er over:
Beskriver krav til når sikkerhetshendelsen er over. Hvis sikkerhetshendelsen var at datanettverket var nede, kan sikkerhetshendelsen være ferdig håndtert når nettverket er tilbake til normal drift.

9. Etter sikkerhetshendelsen:
Tiltak som gjøres etter at selve sikkerhetshendelsen er håndtert og normal drift er gjenopprettet. Slike tiltak kan inkludere steg for å forhindre at sikkerhetshendelsen gjentas, debriefing av ansatte, drøfting av planen (Fungerte den som den skulle? Er det nødvendig med endringer for at den skal fungere optimalt?)

Informasjonen er hentet fra NIST 800-34 [9] og Principles of Incident Response and Disaster Recovery [3].

6.Øvelser og opplæring

Ved å teste planer, trene på sikkerhetshendelser, og å holde øvelser vil personalet være drillet i fremgangsmåter dersom en sikkerhetshendelse skulle oppstå. Man vil betydelig øke effektiviteten i hendelseshåndteringsarbeidet, og dermed også redusere kostanden.

Bevisstgjøring er viktig, og kan også sies å være et forebyggende tiltak. Dersom det jobbes mot sikkerhet og hendelseshåndtering innad i virksomheten, så vil dette føre til at de ansatte ser på det som en del av hverdagen deres, og vil igjen kunne håndtere en gitt sikkerhetshendelse med mye høyere effektivitet. Det at de ansatte er bevisste på eventuelle sikkerhetshendelser vil også hjelpe til å oppdage sikkerhetshendelser ved et tidligere tidspunkt, som igjen kan spare virksomheten for en eskalering av sikkerhetshendelsen.

Totalt mangler 1 av 3 virksomheter retningslinjer for ansattes bruk av virksomhetens IT-løsninger.
- Hentet fra mørketallsundersøkelsen 2008

(Setninger og punkter merket i tykk skrift er minimumskrav, uavhengig av bransje eller størrelse på virksomhet)

- **Opplæring i riktig bruk av informasjonsbehandlingsutstyr, f.eks innloggingsprosedyrer, bruk av programvarepakker og informasjon om disiplinære prosesser er viktig.**

- **Øving sørger for at ansatte er klar over rutiner for hva som skal gjøres i gitte situasjoner**
- Testing sørger for at de automatiserte systemene fungerer som de skal ved en sikkerhetshendelse
- Øving sørger for at underretning fungerer utifra planene.

Selv den minste test, øvelse eller trening vil styrke virksomheten i forkant av en sikkerhetshendelse. Det bør også bestemmes hvilke typer øvelser som er ønskelige å gjennomføre. Dette kan være alt fra full driftstans øvelser til gjennomgang av rutine dokumenter. Mer informasjon rundt øvelser og opplæring finner du her [12].

7. Vedlikehold av plan

For å kunne vedlikeholde en hendelseshåndteringsplan kreves det revisjoner. Revisjoner skal være planlagte og skal innebære en komplett gjennomgang av planen. Dersom en sikkerhetshendelse oppstår skal man i etterkant gå igjennom planen og gjøre eventuelle forandringer som følge av erfaringer lært fra forenstående sikkerhetshendelse.

(Setninger og punkter merket i tykk skrift er minimumskrav, uavhengig av bransje eller størrelse på virksomhet)

Viktige punkter for vedlikehold av plan:

- **Gå igjennom planer, og revider de minst en gang i året**
- Loggføre alle revisjoner
- Gå igjennom planer etter store endringer i virksomheten
- Gå igjennom planer etter endte sikkerhetshendelser;
  - Fungerte alt som det skulle?

Mer informasjon rundt vedlikehold av plan kan du finne i NIST 800-34 [9].

8. Outsourcing

Med ”outsourcing” mener vi en tredjepart på kontrakt utfører en tjeneste for en virksomhet. En prosess som ofte innebærer at tredjeparten får tilgang på informasjon, data eller fysisk tilgang hos virksomheten.

Det viktigste å ha på plass når man vurderer å outsource er å ha en klar avtale rundt hva outsourcingen innebærer, og hvordan den skal foregå. Det er helt opp til deg som eier av informasjonen å være forsikret om at den du outsourcer til har tilstrekkelige planer og sikkerhet. Når man utformer avtalen mellom din virksomhet og databehandler bør man stille seg følgende spørsmål:

(Setninger og punkter merket i tykk skrift er minimumskrav, uavhengig av bransje eller størrelse på virksomhet)

- **Kvalitet på tjeneste, og forventet fremtidig kvalitet.**
- **Hvordan fordeles ansvaret**
- **Sensitiv informasjon deles med databehandler det outsources til, hvordan forholder du deg til dette?**
- Kunnskap om databehandler, og hvordan data blir oppbevart, har vi kontroll på dette?
- Outsourcing kan medføre tregere reaksjon på sikkerhetshendelser, hvordan skal dette håndteres?
- Personopplysningsloven [7]

Her [6] finner du hvordan du kan jobbe for beskyttelse av personopplysninger

Hvordan blir eventuelle hendelser rapportert til dere? Hvordan vil de ansatte i din virksomhet rapportere sikkerhetshendelser til de som drifter systemene deres? Sørg for å avtale statusmøter hvor databehandler rapporterer om sikkerhetshendelser, eller angrep som har oppstått den siste tiden.

Når det kommer til utvikling av avtalen, sammarbeid gjerne med databehandler, på den måten oppstår det ingen uklarheter ved senere annledninger.

9. Eksempler på trusselscenarioer

Du anser kanskje deg og din virksomhet som tilstrekkelig sikret i form av hendelseshåndterings arbeid, og føler virksomheten er kompetent til å håndtere de fleste utfordringer. Her er det listet noen trusselscenarioer, og det er viktig at du spør deg selv; Er jeg og min virksomhet forberedt på dette?

- Det har vært innbrudd i virksomhetens lokaler over helgen, det mangler to servere og halvparten av klientene er borte.
- Lokasjonen hvor du har backup er utsatt for brann. Har du backup på flere lokasjoner?
- Du oppdager at flere viktige filer i virksomhetens datasystemer har blitt forandret, og det på unormale tider av døgnet.
- Du har mistanke om en utro tjener.

- Det har oppstått vannlekasje i virksomhetens lokaler.
- Virksomhetens IT nettverk har blitt utsatt for et kraftig virus angrep.
- En av de ansatte pådrar seg alvorlige personskader under arbeidstiden.

Når man har gode policyer, planer og rutiner, så skal det ikke eksistere nøling ved hva man skal foreta seg ved disse gitte scenarioene. Det kan være en utfordring å finne hvilke trusler som er reelle for din virksomhet, gjør nøye vurderinger og sørg for å være oppdatert.

Husk at sikkerhet er en kontinuerlig prosess, lykke til.

Referanser:

[1]. Mørketallsundersøkelsen 2003 (NorSIS, Økokrim, Næringslivets sikkerhetsråd)
[2]. Mørketallsundersøkelsen 2008 (Næringslivets sikkerhetsråd med flere)
[3]. Principles of Incident Response and Disaster Recovery – Whitman & Mattord 2007.
[4]. NorSIS (Norsk senter for informasjonsikring)
[5]. NSM (Nasjonal sikkerhetsmyndighet)
[6]. Datatilsynet
[7]. Lovdata
[8]. ISO 18044:2004 (Information technology, Security techniques, Information security incident management)
[9]. NIST 800-34:2002 (NIST – Marianne Swanson med flere)
[10]. NS 27002 :2005 (Norsk Standard – Informasjonsteknologi, Sikkerhetsteknikk, Administrasjon av informasjonssikkerhet)
[11]. NS 27005:2008 (Norsk Standard – Informasjonsteknologi, Sikkerhetsteknikk, Styringssystemer for informasjonssikkerhet)
[12]. NIST (National Institute of Standards and Technology)
[13]. Infosecwriters
[14]. Mørketallsundersøkelsen 2006(Næringslivets sikkerhetsråd med flere)

B Vedlegg: Questback spørreundersøkelse

HENDELSESHÅNDTERING

Dette er en spørreundersøkelse angående hendelseshåndtering i norske virksomheter. Undersøkelsen består av 24 spørsmål.

Din identitet vil holdes skjult
Les om skjult identitet her...

1) Hvor mange ansatte er det i din virksomhet?

1-20
21-100
Over 100

2) Hvilken sektor tilhører din virksomhet?

Bank, finans, forsikring
Kjemikalier, helse
Energi, kraft
Industri/produksjon
Media, post
Prossesindustri
Offentlig sektor
Detaljhandel
Leverandør av IT-tjenester
Telekommunikasjon
Transport
Annet

POLICY

3) Har din virksomhet en informasjonssikkerhetspolicy?

Ja
Nei
Vet ikke

4) Dekker denne policyen hendelseshåndtering?

Ja
Nei
Vet ikke

5) Har din virksomhet en egen hendelseshåndteringspolicy?

Ja
Nei
Vet ikke

6) Beskriver informasjonssikkerhetspolicyen eller hendelseshåndteringspolicyen hva en sikkerhetshendelse er?

Ja
Nei
Vet ikke

OPPLÆRING

7) Som en del av opplæringen, har dere gjennomgang av (Flervalg):

Informasjonssikkerhetspolicy
Hendelseshåndteringspolicy
Hendelseshåndteringsplaner
Vet ikke

8) Har virksomheten kursing / opplæring vedrørende hendelseshåndtering for ledelsen?

Ja
Nei
Vet ikke

9) Utfører virksomheten øvelser basert på hendelseshåndteringsplanene?

Ja
Nei
Vet ikke

RAPPORTERING

10) Har virksomheten rutiner for å rapportere sikkerhetshendelser?

Ja
Nei
Vet ikke

11) Har dere rutiner for anonym rapportering (varsling) av sikkerhetshendelser?

Ja
Nei
Vet ikke

12) Dersom det skulle oppstå en sikkerhetshendelse, vet de ansatte hvem de skal kontakte?

Ja
Nei
Vet ikke

13) Er det klare rutiner på plass dersom det skulle være behov for ekstern kontakt? (brannvesen, politi etc...)

Ja
Nei

Vet ikke

14) Hvor mange sikkerhetshendelser ble registrert i din virksomhet i 2009?

Vet ikke
5 eller mindre
6-25
26-50
51+

15) Hvor mange av de registrerte hendelsene ble rapportert videre til ledelsen?

Vet ikke
5 eller mindre
6-25
26-50
51+

Hendelseshåndtering

16) Har dere satt av midler til håndtering av sikkerhetshendelser?

Ja
Nei
Vet ikke

17) Har dere dedikert personell som håndterer sikkerhetshendelser?

Ja
Nei
Vet ikke

18) Etter endt hendelse...

	Ja	Nei	Vet ikke
Har virksomheten noen rutiner for å finne ut om hendelseshåndteringsplanen fungerte?			
Har virksomheten rutiner for revisjon av hendelseshåndteringsplan?			
Har virksomheten rutiner for debriefing av ansatte?			

19) Har dere installert noen form for IDS (intrusion detection system) for å oppdage tekniske sikkerhetshendelser, som for eksempel et hackerangrep?

Ja
Nei
Vet ikke

20) Har din virksomhet rutiner for å vurdere risikoer?

Ja
Nei
Vet ikke

21) Har din virksomhet rutiner for å vurdere virksomhetens verdier?

Ja
Nei
Vet ikke

22) Har din virksomhet beskrevet konsekvenser hvis sikkerhetsregler blir brutt?

Ja
Nei
Vet ikke

23) Dersom din virksomheten blir utsatt for et angrep som er av slik alvorlighetsgrad at det må håndteres ...

	(Dårlig) 1	2	(Middels) 3	4	(Bra) 5
I hvor stor grad vet du hva du skal gjøre?					
I hvor stor grad tror du at medarbeiderne dine vet hva de skal gjøre?					
Hvor godt tror du virksomheten i sin helhet kommer til å håndtere hendelsen?					

24) Fyll inn e-post adressen din her dersom du ønsker resultatet av spørreundersøkelsen og en veileder for hendelseshåndtering.

C Vedlegg: Vedlegg til spørreundersøkelse

Spørreundersøkelse vedrørende hendelseshåndtering i norske virksomheter

Vi er en gruppe på tre studenter ved bachelorstudiet i informasjonssikkerhet på Høgskolen i Gjøvik. Som avslutning på vårt 3-årige studium er vi nå i ferd med å skrive en bacheloroppgave. Oppdragsgiver for oppgaven er Norsk senter for informasjonssikring (NorSIS), og oppgaven går ut på å studere hendelseshåndtering i norske virksomheter.

En viktig del av oppgaven er å dokumentere hvordan hendelseshåndteringsarbeidet utføres i dag, og vi utfører derfor en spørreundersøkelse blant norske virksomheter. Det er i denne sammenheng vi tar kontakt med dere. Hvis dere følger vedlagt lenke vil dere komme til en spørreundersøkelse. Vi håper at dere tar dere tid til å svare, da vi trenger deres hjelp for å få et best mulig resultat.

Prosjektet kommer til å resultere i en rapport og en veiledning for å forenkle implementeringen av en hendelseshåndteringsplan. All informasjon dere oppgir vil bli håndtert konfidensielt, og i oppgaven vil dataene være anonymisert og i hovedsak presenteres i form av statistikk. Som takk for at dere deltar i spørreundersøkelsen vil dere få mulighet til å få tilsendt en kopi av rapporten.

Lenke til undersøkelsen finner du her: Undersøkelse

Har du eventuelle spørsmål til undersøkelsen eller hvis det skulle oppstå problemer kan du kontakte Lars Arne Sand på telefon 97 50 58 99 eller på e-post lars.arne.sand@norsis.no.

På forhånd takk

Mvh
Lars Arne Sand
Anders Sand Frogner
Gaute Wangen

D Vedlegg: Dybdeintervju spørsmål

Spørsmål til dybdeintervju

Totalt 53 spm

GENERELLE SPM:

1. Hvilken sektor tilhører din virksomhet?

2. Hvor mange ansatte er det i din bedrift?

3. Hvilke trusler står din bedriften overfor?

4. Hvordan definerer virksomheten din en hendelse?

5. Har bedriften en CISO (chief of information security)? *Hvis nei, stryk 6 og 7*
6. Er CISO en egen stilling?
7. Hvis ikke, hvilken stilling er kombinert med CISO?

8. Hvilke andre sikkerhetsrelaterte stillinger finnes i virksomheten din?

HYPOTESE 1:

1. Har virksomheten din en informasjonssikkerhetspolicy?

2. Har virksomheten din en hendelseshåndteringspolicy (eller HH som en del av infosek policy)? *Hvis nei, stryk spm 3-8*
   -Har dere noen gang tatt i bruk eller har hatt nytte av hendelseshåndteringspolicyen?
   -Hvorfor ble den sist tatt i bruk?
3. Har HH-policyen et klart definert omfang?
   - Hva omfatter den?
4. Inneholder den klart fordelte roller? (hvis det skulle oppstå en hendelse)
   -Hvilke roller fordeles?
5. Fordeler HH-policyen ansvar?
   -Hvilke stillinger får tildelt ansvarsroller?
6. Er denne hendelseshåndteringspolicyen underskrevet og støttet av en i toppledelsen?
7. Hvor ofte blir denne revidert?

HYPOTESE 2:

1. Går dere gjennom informasjonssikkerhetspolicy som en del opplæringen?
   - Hvor lang tid brukes på det?

2. Hvis dere har en HH policy, går dere gjennom den som en del av opplæringen?

3. Har dere satt av en del av budsjettet til HH opplæring?
   hendelser
4. Har dere opplæring for å håndtere? *Hvis nei, stryk spm 5,6,7,8*
5. Hvilken type opplæring utfører bedriften?
6. Hvor ofte utføres opplæring?

7. Blir det da repetert for de øvrige ansatte?
8. Har dere opplæring for ledelsen?

9. Har dere noen form for revisjon av opplæringsplaner?

HYPOTESE 3:

1. Har virksomheten hendelseshåndteringsplaner? *Hvis nei, stryk spm 2-9*
2. Blir disse planene fulgt under sikkerhetshendelser?
   - Når ble de sist tatt i bruk?
3. Har HH-planen en trigger som gjør at den blir tatt i bruk?
   -isåfall gi et eksempel på en slik?
4. Hvordan fordeler HH-planen ansvar?
5. Hva dekker HH-planen? (omfang)
6. Har HH-planen klart fordelte roller (vet du hva din rolle er under en hendelse)?
7. Hva sier planen om hvordan underretning skal utføres?
8. Blir HH planen revidert etter en sikkerhetshendelse?
   - hvis ikke, hvor ofte blir HH-planen revidert?
9. Utfører virksomheten øvelser basert på hendelseshåndteringsplanene / -policy?
   - når utførte dere sist en slik øvelse?

10. Har bedriften din utført en verdivurdering(BIA)?

HYPOTESE 4:

1. Hvilke ikke-tekniske metoder finnes for å rapportere hendelser?

2. Hvilke tekniske metoder finnes for å rapportere hendelser?

3. Fører dere statistikk på sikkerhetshendelser?

4. Hvordan foregår rapportering hvis det oppstår en hendelse?

5. Rapporteres sikkerhetshendelser til ledelsen?

6. Hvor mange hendelser ble registrert i 2009?

7. Hvor mange av disse ble rapportert til ledelsen?

8. Mener du at bedriften tok de nødvendige stegene i etterkant av hendelsen?

HYPOTESE 5:

1. Hvis det oppdages en hendelse, hvilke tiltak blir satt i gang?

2. Hvilke konsekvenser finnes hvis ansatte ikke følger planen i løpet av en hendelse?

3. Hvordan debriefer virksomheten din i etterkant av en hendelse?

4. Har din virksomhet rutiner for å ta regelmessig backup av IT systemene?

5. Har din virksomhet rutiner for å få systemene tilbake til normal drift (vha backup)?

AVSLUTTENDE SPØRSMÅL:

1. Hva tror du fungerer bra i din bedriften under en hendelse?
2. Hva tror du fungerer mindre bra under en hendelse?
3. Hvis du skulle utviklet en hendelsesteringsplan, hva slags veiledning kunne du tenkt deg?
4. Hvilket format ville du foretrukket å hatt veiledningen i?
5. Hvilken e-post adresse kan vi kan sende rapporten vår til for godkjenning?

E Vedlegg: Spørreundersøkelse deskriptiv statistikk

Deskriptiv statistikk spørreundersøkelse

Spørsmål/svaralternativer	1-20 Liten	21-100 Mellomstor	Over 100 Stor	Svarte ikke
Hvor mange ansatte er det i din virksomhet?	27	14	12	1

Svaralternativer/spørsmål	Hvilken sektor tilhører din virksomhet?
Finans	1
Helse	1
Energi	0
Industri	7
Media	1
Prosess industri	0
Offentlig	7
Handel	2
IT	23
Tele	0
Transport	0
Annet	12

Spørsmål/svaralternativer	Ja	Nei	Vet ikke	Svarte ikke
Har din virksomhet en informasjonssikkerhetspolicy?	37	14	3	0
Dekker denne policyen hendelseshåndtering?	26	19	6	3
Har din virksomhet en egen hendelseshåndteringspolicy?	26	22	5	1
Beskriver informasjonssikkerhetspolicyen eller hendelseshåndteringspolicyen hva en sikkerhetshendelse er?	25	20	7	2

Som en del av opplæringen, har dere gjennomgang av:		
Spørsmål/svaralternativer	Ja	Nei/svarte ikke
Informasjonssikkerhetspolicy	31	23
Hendelseshåndteringspolicy	19	35
Hendelseshåndteringsplaner	13	41
Vet ikke	12	42

Spørsmål/svaralternativer	Ja	Nei	Vet ikke	Svarte ikke
Har virksomheten kursing / opplæring vedrørende hendelseshåndtering for ledelsen?	19	27	8	0
Utfører virksomheten øvelser basert på hendelseshåndteringsplanene?	13	37	4	0
Har virksomheten rutiner for å rapportere sikkerhetshendelser?	27	21	3	3
Har dere rutiner for anonym rapportering (varsling) av	12	36	4	2

sikkerhetshendelser?				
Dersom det skulle oppstå en sikkerhetshendelse, vet de ansatte hvem de skal kontakte?	45	5	4	0
Er det klare rutiner på plass dersom det skulle være behov for ekstern kontakt? (brannvesen, politi etc...)	40	13	0	1

Spørsmål/svaralternativer	Vet ikke	5 eller mindre	6-25	26-50	51+
Hvor mange sikkerhetshendelser ble registrert i din virksomhet i 2009?	21	26	5	1	1
Hvor mange av de registrerte sikkerhetshendelsene ble rapportert videre til ledelsen?	21	28	4	0	1

Spørsmå/svaralternativer	Ja	Nei	Vet ikke	Svarte ikke
Har dere satt av midler til håndtering av sikkerhetshendelser?	20	25	9	0
Har dere dedikert personell som håndterer sikkerhetshendelser?	33	17	2	2
Etter sikkerhetshendelse: Har virksomheten noen rutiner for å finne ut om hendelseshåndteringsplanen fungerte?	24	20	10	0
Etter sikkerhetshendelse: Har virksomheten rutiner for revisjon av hendelseshåndteringsplan?	23	21	10	0
Etter sikkerhetshendelse: Har virksomheten rutiner for debriefing av ansatte?	14	28	12	0
Har dere installert noen form for IDS (intrusion detection system) for å oppdage tekniske sikkerhetshendelser, som for eksempel et hackerangrep?	31	15	7	1
Har din virksomhet rutiner for å vurdere risikoer?	37	13	4	0
Har din virksomhet rutiner for å vurdere virksomhetens verdier?	28	14	10	2
Har din virksomhet beskrevet konsekvenser hvis sikkerhetsregler blir brutt?	24	22	8	0

Dersom din virksomhet blir utsatt for et angrep som er av en slik alvorlighetsgrad at det må håndteres…					
Spørsmål/svaralternativer	1 Dårlig	2	3 Middels	4	5 Bra
I hvor stor grad vet du hva du skal gjøre?	5	3	12	17	17
I hvor stor grad tror du at medarbeiderne dine vet hva de skal gjøre?	7	5	21	13	8
Hvor godt tror du virksomheten i sin helhet kommer til å håndtere sikkerhetshendelsen?	4	1	16	22	11

F Vedlegg: Spørreundersøkelse korrelasjonsanalyse

Spørreundersøkelse korrelasjonsanalyse

Positiv korrelasjon

Ingen spørsmålspar som har korrelasjon over 0.9.

2 Spørsmålspar har korrelasjon over 0.8.

Spørsmålspar	Korrelasjon
4&6	0.8128167
17&18	0.8723737

5 Spørsmålspar som har korrelasjon over 0.7.

Spørsmålspar	Korrelasjon
21&22	0.7845336
22&23	0.7732589
28&29	0.7495717
28&30	0.7909135
29&30	0.7897005

2 Spørsmålspar som har korrelasjon over 0,6.

Spørsmålspar	Korrelasjon
3&5	0.6244921
4&5	0.6008868

32 Spørsmålspar som har korrelasjon over 0,5.

Spørsmålspar	Korrelasjon
3&4	0.5220271
3&6	0.5473366
5&6	0.5230715
6&15	0.5645778
7&28	0.5551795
11&12	0.518972
11&23	0.5364958
21&23	0.5873596

Negativ korrelasjon

2 Spørsmålspar som har korrelasjon under -0,6.

Spørsmålspar	Korrelasjon
3&7	-0.6051435
7&10	-0.6205588

Svaralternativene for 3&7 og 7&10 er satt opp motsatt. Dvs. at en positive svaralternativer har motsatt rekkefølge hos spørsmålene. Det er dermed ikke negativ korrelasjon for disse, men positiv.

5 Spørsmålspar som har korrelasjon under -0,5.

Spørsmålspar	Korrelasjon
5&7	-0.5918269
5&8	-0.5055978
6&7	-0.561677
17&21	-0.5642163
18&21	-0.5146341

Svaralternativene for 5&7, 5&8 og 6&7 er satt opp motsatt. Dvs. at en positive svaralternativer har motsatt rekkefølge hos spørsmålene. Det er dermed ikke negativ korrelasjon for disse, men positiv.

G Vedlegg: Spørreundersøekelse ANOVA analyse

Spørreundersøkelse ANOVA-analyse

Etter størrelse

Parameter	**Spørsmål**	**Signifikans**	**Signifikans i %**
Stor	Har informasjonssikkerhetspolicy	0.05615	94,4%
Kommentar: Boxplot av spørsmålet om virksomheten har infomasjonssikkerhetspolicy, viste at store virksomheter var flinkere på dette. Dette bekreftet anova analysen, med en signifikans på 94,4%.			

Parameter	**Spørsmål**	**Signifikans**	**Signifikans i %**
Stor	Har definert sikkerhetshendelse	0.07847	92,2%
Kommentar: Boxplot av spørsmålet om virksomheten hadde definert sikkerhetshendelse viste at store virksomheter var flinkere på dette. Dette bekrefter anova analysen, med en signifikans på 92,2%.			

Parameter	**Spørsmål**	**Signifikans**	**Signifikans i %**
Små og mellomstore	Har øvelser basert på hendelseshåndteringsplanene.	0.02257	97,7%
Kommentar: Boxplot av spørsmålet om virksomheten hadde øvelser basert på hendelseshåndteringsplanene viste at små og mellomstore virksomheter var dårligere på dette. Dette bekrefter anova analysen, med en signifikans på 97,7%.			

Parameter	**Spørsmål**	**Signifikans**	**Signifikans i %**
Store	Har anonym rapportering.	0.08548	91,5%
Kommentar: Boxplot av spørsmålet om virksomheten hadde anonym rapportering viste at store virksomheter var flinkere på dette. Dette bekrefter anova analysen, med en signifikans på 91,5%.			

Etter sektor

Parameter	**Spørsmål**	**Signifikans**	**Signifikans i %**
Offentlig	Har informasjonssikkerhetspolicy.	0.0759	92,4%
Kommentar: Boxplot av spørsmålet om virksomheten hadde informasjonssikkerhetspolicy viste at offentlige virksomheter var flinkere på dette. Dette bekrefter anova analysen, med en signifikans på 92,4%.			

Parameter	**Spørsmål**	**Signifikans**	**Signifikans i %**
Offentlig	Har hendelseshåndteringspolicy.	0.0759	92,4%.
Kommentar: Boxplot av spørsmålet om virksomheten hadde hendelseshåndteringspolicy viste at offentlige virksomheter var flinkere på dette. Dette bekrefter anova analysen, med en signifikans på 92,4%.			

Parameter	**Spørsmål**	**Signifikans**	**Signifikans i %**
Offentlig	Har øvelser basert på hendelseshåndteringsplanene.	0.003161	99,7%

Kommentar: Boxplot av spørsmålet om virksomheten hadde øvelser basert på hendelseshåndteringsplanene viste at offentlige virksomheter var flinkere på dette. Dette bekrefter anova analysen, med en signifikans på 99,7%.

Parameter	**Spørsmål**	**Signifikans**	**Signifikans i %**
Industri	Under en sikkerhetshendelse, i hvor stor grad vet du hva du skal gjøre?	0.02196	97,8%
Kommentar: Boxplot av spørsmålet i hvor stor grad vet du hva du skal gjøre, dersom det oppstår en sikkerhetshendelse, viste at industri hadde mindre tro på seg selv. Dette bekrefter anova analysen, med en signifikans på 97,8%.			

H Vedlegg: Dybdeintervju deskriptiv statistikk

Deskriptiv statistikk dybdeintervju

Svaralternativer/spørsmål	Hvilken sektor tilhører din virksomhet?
Finans	1
Helse	0
Energi	0
Industri	4
Media	1
Prosess industri	1
Offentlig	0
Handel	5
IT	2
Tele	0
Transport	0
Annet	1

Spørsmål/svaralternativer	1-20 Liten	21-100 Mellomstor	Over 100 Stor
Hvor mange ansatte er det i din virksomhet?	8	5	2

Spørsmål/svaralternativer	Ja	Delvis	Nei
Har virksomheten en sjef for informasjonssikkerhet (CISO).	3	5	7
Har virksomheten andre sikkerhetsrelaterte stillinger.	7	2	6
Har virksomheten en informasjonssikkerhetspolicy.	7	1	7
Har virksomheten en policy som dekker hendelseshåndtering.	8	3	4
Er hendelseshåndteringspolicyen tilstrekkelig.	6	4	5
Er hendelseshåndteringspolicyen underskrevet av en i toppledelsen.	9	0	6
Blir den tilstrekkelig revidert (Ja<=årlig, delvis<=3 år, nei=aldri).	8	2	5
Har virksomheten opplæring på hendelseshåndtering.	11	3	1
Er opplæringen tilstrekkelig.	6	7	2
Utfører virksomheten årlig opplæring og repetisjon for alle ansatte.	7	3	5
Blir opplæringsplanene revidert årlig.	7	1	7
Har virksomheten hendelseshåndteringsplaner.	9	2	4
Blir disse planene brukt under sikkerhetshendelser.	9	2	4
Finnes det en trigger for når planen blir tatt i bruk.	8	2	5
Er ansvarsroller fordelt.	7	4	4
Har den et klart definert omfang.	6	5	4
Finnes det rutiner for å revidere hendelseshåndteringsplaner eller revidering etter sikkerhetshendelser.	6	1	8
Beskriver den hvordan varsling skal utføres.	10	1	4
Har virksomheten vurdert hvordan sikkerhetshendelser påvirker virksomheten (BIA).	5	4	6
Finnes det ikke-tekniske metoder for å registrere sikkerhetshendelser.	11	2	2
Finnes det tekniske metoder for å registrere sikkerhetshendelser.	13	1	1
Finnes det metoder for å registrere sikkerhetshendelser.	10	3	2

Samles sikkerhetshendelser i statistikk.	9	0	6
Rapporteres sikkerhetshendelser til ledelsen.	12	3	0
Dersom det oppdages en sikkerhetshendelse, gjøres det noe med den.	11	3	1
Finnes det klare konsekvenser for de ansatte dersom de ikke følger planen i løpet av en sikkerhetshendelse.	5	4	6
Utfører virksomheten debriefing i etterkant av en sikkerhetshendelse.	9	3	3

Hva tror du fungerer bra i din virksomhet under en sikkerhetshendelse?	Hva tror du fungerer mindre bra i din virksomhet under en sikkerhetshendelse
Rapporteringen.	Forbedring av tiltak etter en hendelse.
Samarbeid.	Forståelse og kunnskap om IT.
Erfaring.	Mangel på fagfolk.
Kunnskap.	Kan ta lang tid.
Ansatte.	Krisekommunikasjon.
Rask responstid.	Rapportering av egenskyldte hendelser.
Oppfølging.	Ansatte utsatt ved ran.
Lære av hendelsen.	Ansvarsfordeling.
God fysisk sikkerhet.	Rom for feiltolkning av retningslinjer.
Tidlig varsling	

I Vedlegg: Dybdeintervju korrelasjonsanalyse

Dybdeintervju korrelasjonsanalyse

2 Spørsmålspar som har korrelasjon over 0.9.

Spørsmålspar	Korrelasjon
14&15	0.9117647
14&20	0.9593672

11 Spørsmålspar har korrelasjon over 0.8.

Spørsmålspar	Korrelasjon
6&7	0.8902439
6&9	0.876018
7&9	0.8416644
11&21	0.8346183
14&17	0.8289856
14&18	0.8886426
15&20	0.872152
16&17	0.8277522
17&18	0.8547734
17&20	0.8922374
18&20	0.8658208

13 Spørsmålspar som har korrelasjon over 0.7.

Spørsmålspar	Korrelasjon
3&15	0.7288125
3&18	0.7006437
3&21	0.7824988
7&14	0.7785687
8&21	0.7332132
10&11	0.7126096
10&12	0.7163374
15&16	0.7591941
15&17	0.7368761
15&18	0.793431
16&20	0.7337411
17&19	0.7028694
24&25	0.796003

31 Spørsmålspar som har korrelasjon over 0,6.

Spørsmålspar	Korrelasjon
3&11	0.6437904
3&13	0.6259321
3&14	0.629429

3&16	0.6460874
3&17	0.601734
6&10	0.6984303
6&12	0.6592343
6&14	0.6887339
6&20	0.6570924
7&10	0.6984303
7&12	0.6062601
7&13	0.6466208
7&15	0.6887339
7&20	0.6748516
8&17	0.6864065
8&18	0.6419505
9&10	0.6148367
9&12	0.6300747
9&13	0.6071767
10&14	0.600245
11&12	0.6060952
11&13	0.6089985
13&14	0.6351073
13&15	0.6351073
13&24	0.6727453
14&16	0.6748392
16&18	0.6007618
16&19	0.6436955
18&21	0.6914892
19&20	0.6179846
28&29	0.624695

32 Spørsmålspar som har korrelasjon over 0,5.

Spørsmålspar	Korrelasjon
1&18	0.5478427
3&7	0.5329086
3&9	0.5510746
3&20	0.5501134
3&25	0.5995438
4&28	0.5101743
5&11	0.5074987
6&8	0.573819
6&11	0.5666216
6&13	0.5657932
6&15	0.598899
6&18	0.5299263
7&11	0.5436505
7&17	0.54392
7&18	0.5687014
8&11	0.5204165
8&20	0.5261368

9&11	0.5608174
9&14	0.5904843
9&15	0.5904843
9&16	0.516129
9&20	0.5669817
10&18	0.5089103
10&20	0.5085476
12&13	0.5461643
13&20	0.5492942
13&25	0.5634362
14&19	0.5343698
14&21	0.5689541
15&21	0.5689541
17&21	0.5814317
21&26	0.5466082

1 Spørsmålspar som har korrelasjon under -0,5.

Spørsmålspar	Korrelasjon
1&2	-0.5078828

J Vedlegg: Skript

Script.sh

```
#!/bin/sh

echo "SMB-statistikk script kjorer..."

echo "Script starter vaskeprogram..."
./vaskeprogram
echo "vaskeprogram ferdig..."

echo "Script starter R..."
R --save < kommandoer.R
echo "R ferdig..."
echo "Alle script har kjort, all data er naa ferdig prossesert..."
```

Vaskeprogram.cpp

```
#include <iostream>
#include <fstream>    //For skriving til fil
#include <string.h>   //For string manipulering
using namespace std;
int main() {
  char buffer[100];   //Buffer for innlesing av data
  ifstream innfil("data.csv");   //Leser fra data.csv
  ofstream utfil("r_inn.csv");   //Skriver til r_inn.csv
   if(innfil) {
      innfil >> buffer;           //Leser data
      while(!innfil.eof()) {      //Leser til eof
       if((strcmp("Anonymous",buffer)==0) ||
      (strcmp("identity",buffer)==0)) {     //ser etter stringer
         for(int i=1; i<=30;i++) {     //Går 30 ganger
           innfil >> buffer;     //Leser
           utfil << buffer;      //Skriver
           if(i<30)
           utfil << "\t";
          }
          utfil << "\n";
        }
      innfil >> buffer;
      }
    }
cout << "\n Transformasjon av data er ferdig, dataen kan nå leses av
statistikk programmet R.\n";

return 0;
}
```

Kommandoer.R

```
#INNLESING AV DATA
myData <-
read.table("/home/bruker/Desktop/SMB_statistikk/r_inn.csv",header=FA
LSE,sep="\t",skip=0)
colnames(myData) <-
c("S1","S2","S3","S4","S5","S6","S7","S8","S9","S10","S11","S12","S1
3","S14","S15","S16","S17","S18","S19","S20","S21","S22","S23","S24"
,"S25","S26","S27","S28","S29","S30")
attach(myData)

dataDybde <-
read.table("/home/bruker/Desktop/SMB_statistikk/r_inn_dybdeintervju.
csv",header=FALSE,sep="\t",skip=0)
colnames(dataDybde) <-
c("1","2","3","4","5","6","7","8","9","10","1","12","13","14","15","
16","17","18","19","20","21","22","23","24","25","26","27","28","29"
)

#KOLONNE NAVN SPØRREUNDERSØKELSE
1#1: Hvor mange ansatte er det i din virksomhet?
2#2: Hvilken sektor tilhører din virksomhet?
3#3: Har din virksomhet en informasjonssikkerhetspolicy?
4#4: Dekker denne policyen hendelseshåndtering?
5#5: Har din virksomhet en egen hendelseshåndteringspolicy?
6#6: Beskriver informasjonssikkerhetspolicyen eller
hendelseshåndteringspolicyen hva en sikkerhetshendelse er?
7#7.1: Informasjonssikkerhetspolicy
8#7.2: Hendelseshåndteringspolicy
9#7.3: Hendelseshåndteringsplaner
10#7.4: Vet ikke
11#8: Har virksomheten kursing / opplæring vedrørende
hendelseshåndtering for ledelsen?
12#9: Utfører virksomheten øvelser basert på
hendelseshåndteringsplanene?
13#10: Har virksomheten rutiner for å rapportere
sikkerhetshendelser?
14#11: Har dere rutiner for anonym rapportering (varsling) av
sikkerhetshendelser?
15#12: Dersom det skulle oppstå en sikkerhetshendelse, vet de
ansatte hvem de skal kontakte?
16#13: Er det klare rutiner på plass dersom det skulle være behov
for ekstern kontakt? (brannvesen, politi etc...)
17#14: Hvor mange sikkerhetshendelser ble registrert i din
virksomhet i 2009?
18#15: Hvor mange av de registrerte hendelsene ble rapportert videre
til ledelsen?
19#16: Har dere satt av midler til håndtering av
sikkerhetshendelser?
20#17: Har dere dedikert personell som håndterer
sikkerhetshendelser?
21#18.1: Har virksomheten noen rutiner for å finne ut om
hendelseshåndteringsplanen fungerte?
22#18.2: Har virksomheten rutiner for revisjon av
hendelseshåndteringsplan?
```

23#18.3: Har virksomheten rutiner for debriefing av ansatte?
24#19: Har dere installert noen form for IDS (intrusion detection system) for å oppdage tekniske sikkerhetshendelser, som for eksempel et hackerangrep?
25#20: Har din virksomhet rutiner for å vurdere risikoer?
26#21: Har din virksomhet rutiner for å vurdere virksomhetens verdier?
27#22: Har din virksomhet beskrevet konsekvenser hvis sikkerhetsregler blir brutt?
28#23.1: I hvor stor grad vet du hva du skal gjøre?
29#23.2: I hvor stor grad tror du at medarbeiderne dine vet hva de skal gjøre?
30#23.3: Hvor godt tror du virksomheten i sin helhet kommer til å håndtere hendelsen?

#KOLONNE NAVN DYBDEINTERVJU
#1: Hvilken sektor tilhører virksomheten?
#2: Hvor mange ansatte er det i bedriften?
#3: Har virksomheten en CISO?
#4: Har virksomheten andre sikkerhetsrelaterte stillinger?
#5: Har virksomheten en informasjonssikkerhetspolicy?
#6: Har virksomheten en policy som dekker hendelseshåndtering?
#7: Er hendelseshåndteringspolicyen tilstrekkelig?
#8: Er hendelseshåndteringspolicyen underskrevet av en i toppledelsen?
#9: Blir den tilstrekkelig revidert?
#10: Har virksomheten opplæring på hendelseshåndtering?
#11: Er opplæringen tilstrekkelig?
#12: Utfører bedriften årlig opplæring og repetisjon for alle ansatte?
#13: Blir opplæringsplanene revidert årlig?
#14: Har virksomheten hendelseshåndteringsplaner?
#15: Blir disse planene brukt under sikkerhetshendelser?
#16: Når blir planen tatt i bruk, finnes det en "trigger"?
#17: Er ansvarsroller fordelt?
#18: Har den et klart definert omgang?
#19: Finnes det rutiner for å revidere hendelseshåndteringsplaner eller revidering etter sikkerhetshendelser?
#20: Beskriver den hvordan underretning skal utføres?
#21: Har virksomheten vurdert hvordan sikkerhetshendelsen påvirker virksomheten?
#22: Finnes det ikke-tekniske metoder for å rapportere sikkerhetshendelser?
#23: Finnes det tekniske metoder for å rapportere sikkerhetshendelser?
#24: Finnes det metoder for å registrere sikkerhetshendelser?
#25: Samles sikkerhetshendelser i statistikk?
#26: Rapporteres sikkerhetshendelser til ledelsen?
#27: Dersom det oppdages en sikkerhetshendelse, gjøres det noe med den?
#28: Finnes det klare konsekvenser for de ansatte dersom de ikke følger planen i løpet av en hendelse?
#29: Utfører virksomheten debriefing i etterkant av en hendelse?

#Antall ansatte histogram

```
jpeg("SU_barplot_storrelse.jpg")
antAnsatte<-myData[,c(1)] # Velger bare
aa<-sum(myData[,c(1)]==1)
bb<-sum(myData[,c(1)]==2)
cc<-sum(myData[,c(1)]==3)
temp<-c(aa,bb,cc)
slname=c("Smaa","Mellomstore","Store")
barplot(temp,density=5,col=4,ylab="Antall",names.arg=slname,cex.name
s=1,ylim=c(0,30))
dev.off()

#Hvilken sektor histogram
jpeg("SU_barplot_sektor.jpg")
#sektor<-myData[,c(2)] # Velger bare
aa<-sum(myData[,c(2)]==1)
bb<-sum(myData[,c(2)]==2)
cc<-sum(myData[,c(2)]==3)
dd<-sum(myData[,c(2)]==4)
ee<-sum(myData[,c(2)]==5)
ff<-sum(myData[,c(2)]==6)
gg<-sum(myData[,c(2)]==7)
hh<-sum(myData[,c(2)]==8)
ii<-sum(myData[,c(2)]==9)
jj<-sum(myData[,c(2)]==10)
kk<-sum(myData[,c(2)]==11)
ll<-sum(myData[,c(2)]==12)
temp<-c(aa,bb,cc,dd,ee,ff,gg,hh,ii,jj,kk,ll)
slname<- c("1","2","3","4","5","6","7","8","9","10","11","12")
barplot(temp,density=5,col=4,ylab="Antall",names.arg=slname,cex.name
s=1,ylim=c(0,25))
dev.off()

#Har infosec policy histogram
jpeg("SU_barplot_infosekpolicy.jpg")
infosecPolicy<-myData[,c(3)] # Velger bare
aa<-sum(myData[,c(3)]==1)
bb<-sum(myData[,c(3)]==2)
cc<-sum(myData[,c(3)]==3)
temp<-c(aa,bb,cc)
slname<- c("Ja(68,5%)","Nei(26%)","Vet ikke(5,5%)")
barplot(temp,density=5,col=4,ylab="Antall",names.arg=slname,cex.name
s=1,ylim=c(0,40))
dev.off()

#Definerer sikkerhetshendelse histogram
jpeg("SU_barplot_defSikkerhetshendelse.jpg")
defSikkerhetshendelse<-myData[,c(6)] # Velger bare
slname<- c("Ja(48%)","Nei(38,5%)","Vet ikke(13,5%)")
aa<-sum(myData[,c(6)]==1)
bb<-sum(myData[,c(6)]==2)
cc<-sum(myData[,c(6)]==3)
temp<-c(aa,bb,cc)
barplot(temp,density=5,col=4,ylab="Antall",names.arg=slname,cex.name
s=1,ylim=c(0,30))
dev.off()
```

```
#Som en del av opplæringen, har dere gjennomgang av
jpeg("barplot_opplaeringgjennomgang.jpg")
opplaering<-myData[,c(7:10)] # Velger bare
aa<-sum(myData[,c(7)]==1)
bb<-sum(myData[,c(8)]==1)
cc<-sum(myData[,c(9)]==1)
dd<-sum(myData[,c(10)]==1)
temp<-c(aa,bb,cc,dd)
slname<- c("Infosek policy","HH policy","HH planer","Vet ikke")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,35),names.arg=sl
name,cex.names=1)
dev.off()

#Definerer sikkerhetshendelse histogram
jpeg("SU_barplot_rutinerforrapportering.jpg")
rutinerRapportering<-myData[,c(13)] # Velger bare
aa<-sum(myData[,c(13)]==1)
bb<-sum(myData[,c(13)]==2)
cc<-sum(myData[,c(13)]==3)
temp<-c(aa,bb,cc)
slname<- c("Ja(52,9%)","Nei(41,2%)","Vet ikke(5,9%)")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,35),names.arg=sl
name,cex.names=1)
dev.off()

#Antall registrerte hendelser histogram
jpeg("SU_barplot_antreghendelser.jpg")
antreghendelser<-myData[,c(17)] # Velger bare
aa<-sum(myData[,c(17)]==1)
bb<-sum(myData[,c(17)]==2)
cc<-sum(myData[,c(17)]==3)
dd<-sum(myData[,c(17)]==4)
ee<-sum(myData[,c(17)]==5)
temp<-c(aa,bb,cc,dd,ee)
slname<- c("Vet ikke(38,9%)","<5(48%)","6-25(9,3%)","26-
50(1,9%)","51+(1,9%)")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,30),names.arg=sl
name,cex.names=0.8)
dev.off()

#Etter endt hendelse
jpeg("SU_barplot_etterendthendelse.jpg")
etterendthendelse<-myData[,c(21:23)] # Velger bare
aa<-sum(myData[,c(21)]==1)
bb<-sum(myData[,c(22)]==1)
cc<-sum(myData[,c(23)]==1)
temp<-c(aa,bb,cc)
slname<- c("Finne ut om \n planen fungerte","\nRevisjon av HH
plan","Debriefing av ansatte")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,30),names.arg=sl
name,cex.names=0.9)
dev.off()

#CASE: Etter endt hendelse DU
jpeg("SU_barplot_CaseDu.jpg")
CaseDu<-myData[,c(28)] # Velger bare
```

```
aa<-sum(myData[,c(28)]==1)
bb<-sum(myData[,c(28)]==2)
cc<-sum(myData[,c(28)]==3)
dd<-sum(myData[,c(28)]==4)
ee<-sum(myData[,c(28)]==5)
temp<-c(aa,bb,cc,dd,ee)
slname<- c("1 Daarlig\n(9,3%)","2\n(5,3%)","3
Middels\n(22,2%)","4\n(31,5%)","5 Bra\n(31,5%)")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,25),names.arg=sl
name,cex.names=0.9)
dev.off()

#CASE: Etter endt hendelse MEDARBEIDER
jpeg("SU_barplot_CaseMedarbeider.jpg")
CaseMedarbeider<-myData[,c(29)] # Velger bare
aa<-sum(myData[,c(29)]==1)
bb<-sum(myData[,c(29)]==2)
cc<-sum(myData[,c(29)]==3)
dd<-sum(myData[,c(29)]==4)
ee<-sum(myData[,c(29)]==5)
temp<-c(aa,bb,cc,dd,ee)
slname<- c("1 Daarlig\n(13%)","2\n(9,3%)","3
Middels\n(38,9%)","4\n(24,1%)","5 Bra\n(14,8%)")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,25),names.arg=sl
name,cex.names=0.9)
dev.off()

#CASE: Etter endt hendelse VIRKSOMHETEN
jpeg("SU_barplot_CaseVirksomheten.jpg")
CaseVirksomheten<-myData[,c(30)] # Velger bare
aa<-sum(myData[,c(30)]==1)
bb<-sum(myData[,c(30)]==2)
cc<-sum(myData[,c(30)]==3)
dd<-sum(myData[,c(30)]==4)
ee<-sum(myData[,c(30)]==5)
temp<-c(aa,bb,cc,dd,ee)
slname<- c("1 Daarlig\n(7,4%)","2\n(1,9%)","3
Middels\n(29,6%)","4\n(40,7%)","5 Bra\n(20,4%)")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,25),names.arg=sl
name,cex.names=0.9)
dev.off()



#DYBDEINTERVJU_ANALYSE

#1#Hvilken sektor histogram
jpeg("DI_barplot_sektor.jpg")
DI_sektor<-dataDybde[,c(1)] # Velger bare
aa<-sum(dataDybde[,c(1)]==1)
bb<-sum(dataDybde[,c(1)]==2)
cc<-sum(dataDybde[,c(1)]==3)
dd<-sum(dataDybde[,c(1)]==4)
ee<-sum(dataDybde[,c(1)]==5)
ff<-sum(dataDybde[,c(1)]==6)
gg<-sum(dataDybde[,c(1)]==7)
```

```
hh<-sum(dataDybde[,c(1)]==8)
ii<-sum(dataDybde[,c(1)]==9)
jj<-sum(dataDybde[,c(1)]==10)
kk<-sum(dataDybde[,c(1)]==11)
ll<-sum(dataDybde[,c(1)]==12)
temp<-c(aa,bb,cc,dd,ee,ff,gg,hh,ii,jj,kk,ll)
slname<- c("1","2","3","4","5","6","7","8","9","10","11","12")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,6),names.arg=sln
ame,cex.names=0.9)
dev.off()

#9#HH Policy tilstrekkelig revidert
jpeg("DI_barplot_HHP_revisjon.jpg")
DI_HHPRevidert<-dataDybde[,c(9)] # Velger bare
aa<-sum(dataDybde[,c(9)]==1)
bb<-sum(dataDybde[,c(9)]==2)
cc<-sum(dataDybde[,c(9)]==3)
temp<-c(aa,bb,cc)
slname=c("Aarlig","<=3Aar","Aldri")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,10),names.arg=sl
name,cex.names=0.9)
dev.off()

#10#Opplæring på hendelseshåndtering
jpeg("DI_barplot_HHOpplaering.jpg")
DI_HHOpplaering<-dataDybde[,c(10)] # Velger bare
aa<-sum(dataDybde[,c(10)]==1)
bb<-sum(dataDybde[,c(10)]==2)
cc<-sum(dataDybde[,c(10)]==3)
temp<-c(aa,bb,cc)
slname=c("Ja","Delvis","Nei")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,15),names.arg=sl
name,cex.names=0.9)
dev.off()

#19#HH planer revisjon
jpeg("DI_barplot_HH_Plan_Revisjon.jpg")
DI_HHPlanRevisjon<-dataDybde[,c(19)] # Velger bare
aa<-sum(dataDybde[,c(19)]==1)
bb<-sum(dataDybde[,c(19)]==2)
cc<-sum(dataDybde[,c(19)]==3)
temp<-c(aa,bb,cc)
slname=c("Ja","Delvis","Nei")
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,10),names.arg=sl
name,cex.names=0.9)
dev.off()


#26#Rapporteres sikkerhetshendelser til ledelsen
jpeg("DI_barplot_rapporteres_ledelsen.jpg")
DI_RapporteresLedelsen<-dataDybde[,c(26)] # Velger bare
aa<-sum(dataDybde[,c(26)]==1)
bb<-sum(dataDybde[,c(26)]==2)
cc<-sum(dataDybde[,c(26)]==3)
temp<-c(aa,bb,cc)
slname=c("Ja","Delvis","Nei")
```

```
barplot(temp,density=5,col=4,ylab="Antall",ylim=c(0,15),names.arg=sl
name,cex.names=0.9)
dev.off()
```

Korrelasjonsanalyse.R

```
#INNLESING AV DATA
myData <-
read.table("/home/bruker/Desktop/SMB_statistikk/r_inn.csv",header=FA
LSE,sep="\t",skip=0)
colnames(myData) <-
c("S1","S2","S3","S4","S5","S6","S7","S8","S9","S10","S11","S12","S1
3","S14","S15","S16","S17","S18","S19","S20","S21","S22","S23","S24"
,"S25","S26","S27","S28","S29","S30")
attach(myData)

dataDybde <-
read.table("/home/bruker/Desktop/SMB_statistikk/r_inn_dybdeintervju.
csv",header=FALSE,sep="\t",skip=0)
colnames(dataDybde) <-
c("1","2","3","4","5","6","7","8","9","10","1","12","13","14","15","
16","17","18","19","20","21","22","23","24","25","26","27","28","29"
)

#Korrelasjon sporreundersokelse
dummy<-c(1:30,1:30)
dummy[30,30]
s<-numeric(0)
for (i in 2:30) {
 k=i-1
 for (j in 1:k) {
  z<-cor(myData[i],myData[j])
   if((z>0.5)&(z<1)) s<-rbind(s,c(i,j))
 #   if(z<(-0.5)) s<-rbind(s,c(i,j))
 }
}
s

#Korrelasjon dybdeintervju
dummy<-c(1:29,1:29)
dummy[29,29]
s<-numeric(0)
for (i in 2:29) {
 k=i-1
 for (j in 1:k) {
  z<-cor(dataDybde[i],dataDybde[j])
   if((z>0.5)&(z<1)) s<-rbind(s,c(i,j))
#   if((z<(-0.5))) s<-rbind(s,c(i,j))
 }
}
s
```

Anova.R

```
#INNLESING AV DATA
myData <-
read.table("/home/bruker/Desktop/SMB_statistikk/r_inn.csv",header=FA
LSE,sep="\t",skip=0)
colnames(myData) <-
c("S1","S2","S3","S4","S5","S6","S7","S8","S9","S10","S11","S12","S1
3","S14","S15","S16","S17","S18","S19","S20","S21","S22","S23","S24"
,"S25","S26","S27","S28","S29","S30")
attach(myData)

#ANOVA ANALYSE
#ETTER STORRELSE
jpeg("SU_boxplot_infosekpolicy.jpg")
boxplot(S3~S1) #Viser at nesten alle store virksomheter har
infosekpolicy
dev.off()

dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==3)
 dummy[i]=1
}
anova(lm(S3~factor(dummy)))
#ANALYSEN VISTE 0.05615.

boxplot(S4~S1) #Viser at nesten alle store virksomheter har
infosekpolicy som dekker HH
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==3)
 dummy[i]=1
}
anova(lm(S4~factor(dummy)))
#ANALYSEN VISTE AT INGEN VARIANS

boxplot(S5~S1) #Ikke interressant
boxplot(S6~S1) #Viser at store virksomheter er flinkere pÃ¥ Ã¥
definere S_hendelse
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==3)
 dummy[i]=1
}
anova(lm(S6~factor(dummy)))
#ANALYSEN VISTE 0.07847
```

```
boxplot(S7~S1) #Store virksomheter til en viss grad flinkere med
opplÃ¦ring pÃ¥ infosek policy
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==3)
 dummy[i]=1
}
anova(lm(S7~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS

boxplot(S8~S1) #Ikke interressant
boxplot(S9~S1) #Ikke interressant
boxplot(S10~S1) #Ikke interressant
boxplot(S11~S1) #Mellomstore virksomheter dÃ¥rligere pÃ¥
kursing/opplÃ¦ring for ledelse
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==2)
 dummy[i]=1
}
anova(lm(S11~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS

jpeg("SU_boxplot_ovelse.jpg")
boxplot(S12~S1) #Viser at smÃ¥ og mellomstore virksomheter er klart
dÃ¥rligere pÃ¥ Ã¸velse
dev.off()

dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==2 || myData[i,1]==1)
 dummy[i]=1
}
anova(lm(S12~factor(dummy)))
#ANALYSEN VISTE 0.02257 *

boxplot(S13~S1) #Ikke interressant
boxplot(S14~S1) #Store flinkere pÃ¥ anonym rapportering
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==3)
 dummy[i]=1
}
anova(lm(S14~factor(dummy)))
#ANALYSEN VISTE 0.08548 .

boxplot(S15~S1) #Ikke interressant
boxplot(S16~S1) #Ikke interressant
```

```
boxplot(S17~S1) #Store virksomheter rapporterer fÃ¦rre hendelser
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==3)
 dummy[i]=1
}
anova(lm(S17~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS


boxplot(S18~S1) #Samme som forrige, men til ledelse
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==3)
 dummy[i]=1
}
anova(lm(S18~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS

boxplot(S19~S1) #Ikke interressant
boxplot(S20~S1) #Ikke interressant
boxplot(S21~S1) #Ikke interressant
boxplot(S22~S1) #Ikke interressant
boxplot(S23~S1) #Store flinkere til debriefing av ansatte etter
hendelse
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==3)
 dummy[i]=1
}
anova(lm(S23~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS

boxplot(S24~S1) #Ikke interressant
boxplot(S25~S1) #Ikke interressant
boxplot(S26~S1) #Ikke interressant
boxplot(S27~S1) #Ikke interressant
boxplot(S28~S1) #Bevistheten pÃ¥ hva som skal gjÃ¸res er hÃ¸yere hos
smÃ¥ og mellomstore
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==1 || myData[i,1]==2)
 dummy[i]=1
}
anova(lm(S28~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS

boxplot(S29~S1) #SmÃ¥ og mellomstore har stÃ¸rre tro pÃ¥ kollegaer
```

```
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,1]==1 || myData[i,1]==2)
 dummy[i]=1
}
anova(lm(S29~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS

boxplot(S30~S1) #Alle stÃ¸rrelser svarer likt pÃ¥ hÃ¥ndtering av
hendelse
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS




#ETTER SEKTOR
jpeg("SU_boxplot_sektor_infosekpolicy.jpg")
boxplot(S3~S2) #Offentlig sektor 7 flinkere pÃ¥ infosekpolicy
dev.off()
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==7)
 dummy[i]=1
}
anova(lm(S3~factor(dummy)))
#ANALYSEN VISTE 0.0759 .

boxplot(S4~S2) #Ikke interressant
boxplot(S5~S2) #Offentlig7 flinke pÃ¥ hh policy.
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==7)
 dummy[i]=1
}
anova(lm(S5~factor(dummy)))
#ANALYSEN VISTE 0.0759 .

boxplot(S6~S2) #Ikke interressant
boxplot(S7~S2) #Industri4 dÃ¥rligere pÃ¥ opplÃ¦ring infosekpolicy,
mens offentlig og it er flinke
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==4)
 dummy[i]=1
}
anova(lm(S7~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS
```

```
boxplot(S8~S2) #Ikke interressant
boxplot(S9~S2) #Ikke interressant
boxplot(S10~S2) #Ikke interressant
boxplot(S11~S2) #Offentlig7 flinkere pÃ¥ kursing og opplÃ¦ring
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==7)
 dummy[i]=1
}
anova(lm(S11~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANT VARIANS

jpeg("SU_boxplot_sektor_ovelse.jpg")
boxplot(S12~S2) #Offentlig7 flinkere pÃ¥ Ã¸velser
dev.off()
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==7)
 dummy[i]=1
}
anova(lm(S12~factor(dummy)))
#ANALYSEN VISTE 0.003161 **

boxplot(S13~S2) #Ikke interressant
boxplot(S14~S2) #Ikke interressant
boxplot(S15~S2) #Ikke interressant
boxplot(S16~S2) #Ikke interressant
boxplot(S17~S2) #Ikke interressant
boxplot(S18~S2) #Ikke interressant
boxplot(S19~S2) #Industri4 flinkere til Ã¥ sette av midler til HH.
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==4)
 dummy[i]=1
}
anova(lm(S19~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANS VARIANS

boxplot(S20~S2) #Ikke interressant
boxplot(S21~S2) #Industri4 og offentlig7 flinkere til Ã¥ finne ut om
planen fungerte
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==4 || myData[i,2]==7)
 dummy[i]=1
}
anova(lm(S21~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANS VARIANS
```

```
boxplot(S22~S2) #Industri4 og offentlig7 bedre pÃ¥ rutiner for
revisjon
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==4 || myData[i,2]==7)
 dummy[i]=1
}
anova(lm(S22~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANS VARIANS

boxplot(S23~S2) #Offentlig7 flinkere pÃ¥ debriefing
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==7)
 dummy[i]=1
}
anova(lm(S23~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANS VARIANS

boxplot(S24~S2) #Ikke interressant
boxplot(S25~S2) #Ikke interressant
boxplot(S26~S2) #Offentlig7 dÃ¥rligere pÃ¥ Ã¥ vurdere verdier
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==7)
 dummy[i]=1
}
anova(lm(S26~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANS VARIANS

boxplot(S27~S2) #Industri4 beskriver bedre konsekvenser ved brudd
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==4)
 dummy[i]=1
}
anova(lm(S27~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANS VARIANS

jpeg("SU_boxplot_sektor_casedu.jpg")
boxplot(S28~S2) #Industri4 har mindre tro pÃ¥ seg selv ved en
hendelse
dev.off()
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
```

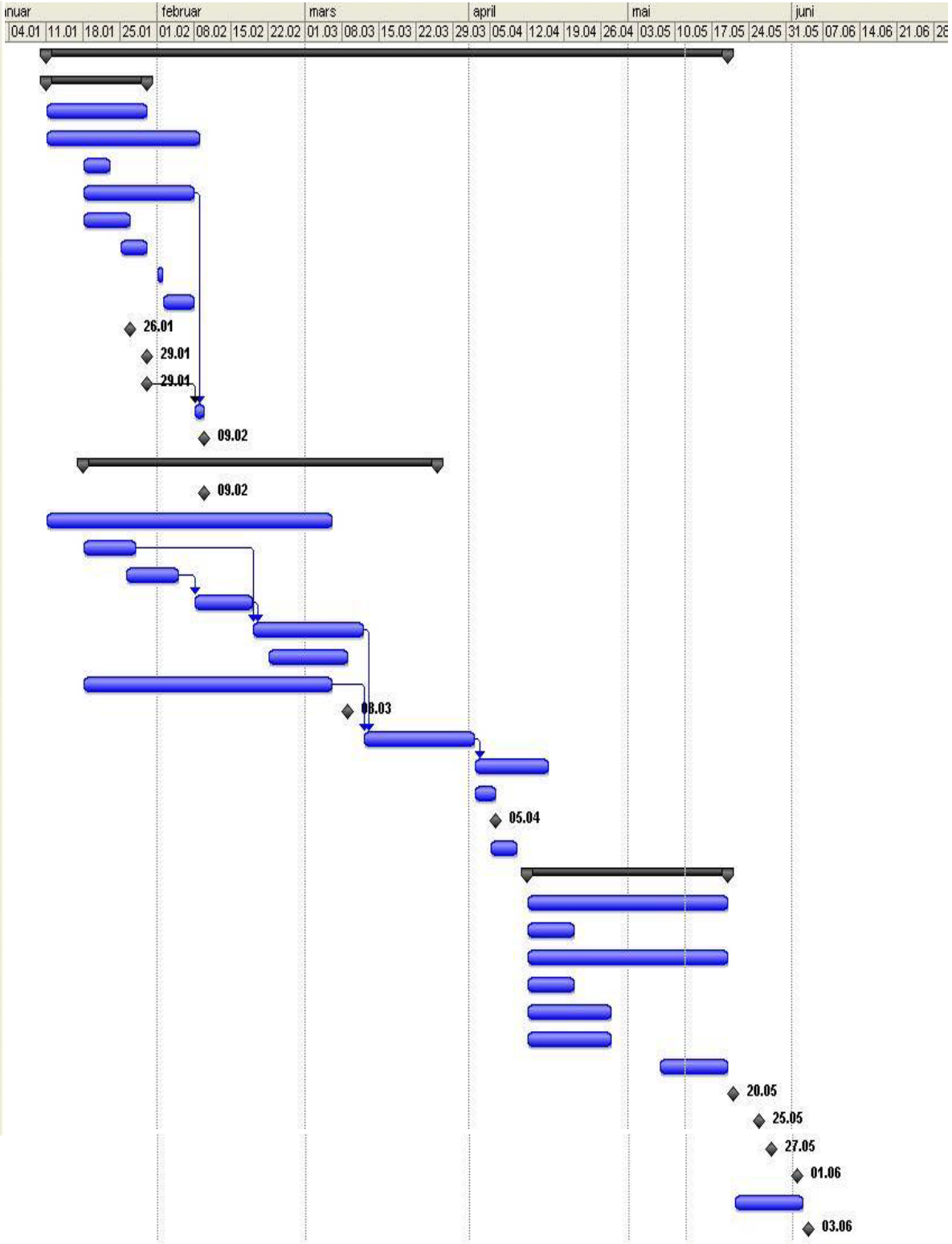
```
 if(myData[i,2]==4)
 dummy[i]=1
}
anova(lm(S28~factor(dummy)))
#ANALYSEN VISTE 0.02196 *

boxplot(S29~S2) #IT har stÃ¸rre tro pÃ¥ medarbeidere
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==9)
 dummy[i]=1
}
anova(lm(S29~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANS VARIANS

boxplot(S30~S2) #IT har stÃ¸rre tro pÃ¥ at virksomheten vil gjÃ¸re
det bra
dummy<-1:54
dummy[1:54]=0
i=0
for (i in 1:54) {
 if(myData[i,2]==9)
 dummy[i]=1
}
anova(lm(S30~factor(dummy)))
#ANALYSEN VISTE INGEN SIGNIFIKANS VARIANS
```

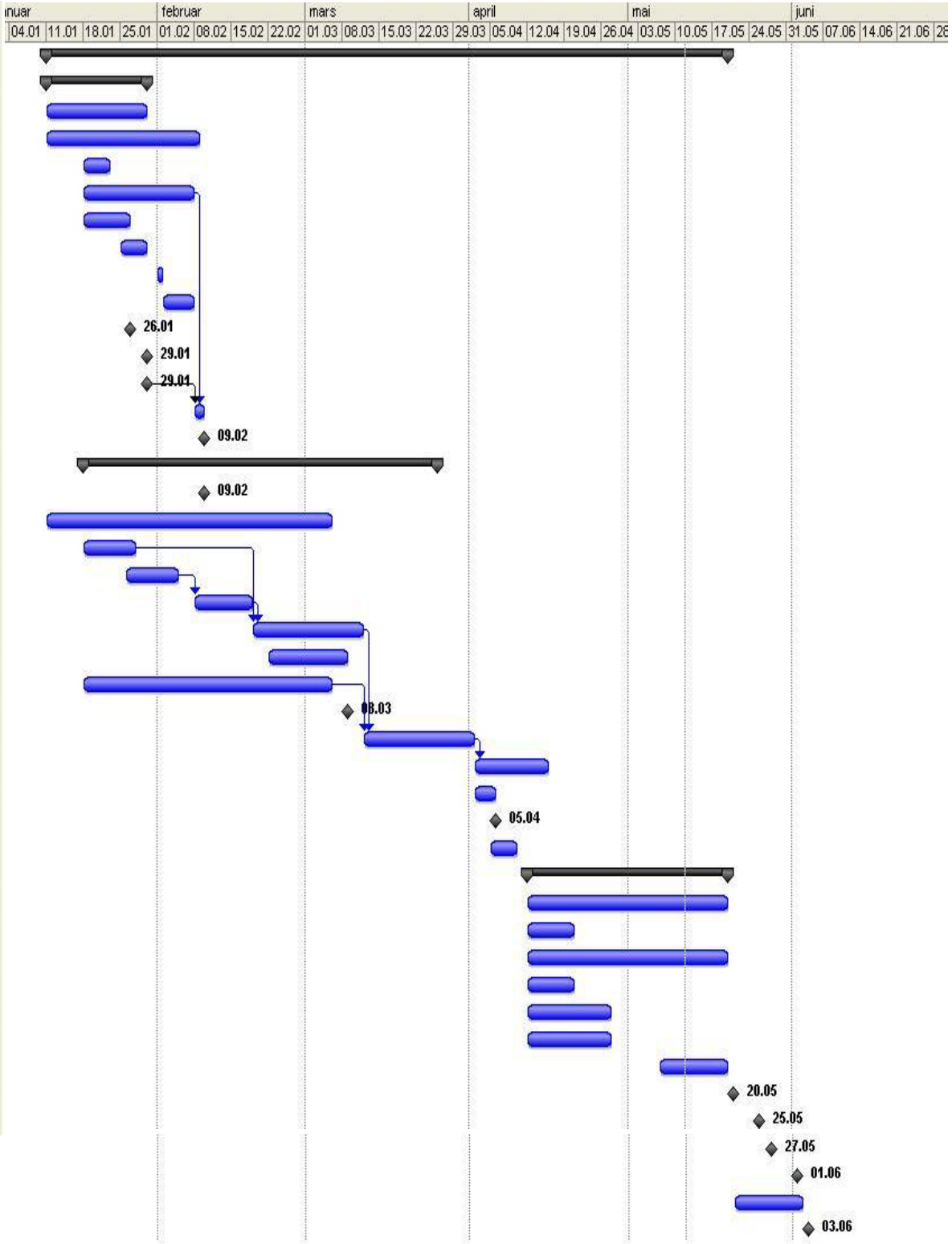
K Vedlegg: Planlagt prosjektplan

	Aktivitetsnavn	Varighet	Start	Slutt
1	Rapportskriving	93 dager	ma 11.01.10	on 19.05.10
2	Forprosjekt	15 dager	ma 11.01.10	fr 29.01.10
3	Arbeide med forprosjekt dokumentet	15 dager	ma 11.01.10	fr 29.01.10
4	Lære LateX	21 dager	ma 11.01.10	ma 08.02.10
5	Utvikle Webside	5 dager	ma 18.01.10	fr 22.01.10
6	Utvikle spørreundersøkelse	15 dager	ma 18.01.10	sø 07.02.10
7	Jobbe med hvilke temaer spørreundersøkelsen skal c	7 dager	ma 18.01.10	ti 26.01.10
8	Finne ut hvilke virksomheter den skal distribueres til	5 dager	ma 25.01.10	fr 29.01.10
9	Test av spørreundersøkelse	1 dag	ma 01.02.10	ma 01.02.10
10	Evaluering og endringer på spørreundersøkelse	4 dager	ti 02.02.10	sø 07.02.10
11	Levere inn forprosjekt til veileder og oppdragsgiver	1 dag	ti 26.01.10	ti 26.01.10
12	Levere inn kontrakt til veileder og oppdragsgiver	1 dag	fr 29.01.10	fr 29.01.10
13	Innleveringsfrist for forprosjekt	1 dag	fr 29.01.10	fr 29.01.10
14	Jobbe med Statusrapport	2 dager	ma 08.02.10	ti 09.02.10
15	Levere statusrapport	1 dag	ti 09.02.10	ti 09.02.10
16	Spørreundersøkelse og Dybdeintervju	49 dager	ma 18.01.10	to 25.03.10
17	Utsending av spørreundersøkelse	2 dager	ma 08.02.10	ti 09.02.10
18	Literaturstudie	40 dager	ma 11.01.10	fr 05.03.10
19	Finne kilder	8 dager	ma 18.01.10	on 27.01.10
20	Finne gjeldende lover og standarder for tema	8 dager	ti 26.01.10	to 04.02.10
21	Analysere viktige lover og standarder	9 dager	ma 08.02.10	to 18.02.10
22	Forberede dybdeintervju	15 dager	fr 19.02.10	to 11.03.10
23	Lære analyse-verktøyet "R"	11 dager	ma 22.02.10	ma 08.03.10
24	Sette seg inn i nødvendig kunnskap for videre arbeid	35 dager	ma 18.01.10	fr 05.03.10
25	Forventet svar på spørreundersøkelse	1 dag	ma 08.03.10	ma 08.03.10
26	Utføre dybdeintervju	15 dager	fr 12.03.10	to 01.04.10
27	Bearbeide data og forberede veiledning	10 dager	fr 02.04.10	to 15.04.10
28	Jobbe med Statusrapport	2 dager	fr 02.04.10	ma 05.04.10
29	Levere Statusrapport	1 dag	ma 05.04.10	ma 05.04.10
30	Påskeferie	5 dager	ma 05.04.10	fr 09.04.10
31	Skrive veiledning og gjøre klart for innlevering	28 dager	ma 12.04.10	on 19.05.10
32	Utvikle veiledning for små bedrifter	28 dager	ma 12.04.10	on 19.05.10
33	Kartlegge behov for små bedrifter	7 dager	ma 12.04.10	ti 20.04.10
34	Utvikle veiledning for mellomstore bedrifter	28 dager	ma 12.04.10	on 19.05.10
35	Kartlegge behov for mellomstore bedrifter	7 dager	ma 12.04.10	ti 20.04.10
36	Analysere data og finne de viktigste aspektene	12 dager	ma 12.04.10	ti 27.04.10
37	Vurdere struktur og oppsett for veiledning	12 dager	ma 12.04.10	ti 27.04.10
38	Forberede innlevering	9 dager	fr 07.05.10	on 19.05.10
39	Levere bachelor oppgaven til kopisentralen	1 dag	to 20.05.10	to 20.05.10
40	Levere bachelor oppgaven til studenttorget	1 dag	ti 25.05.10	ti 25.05.10
41	A3 plakat leveres til laminering	1 dag	to 27.05.10	to 27.05.10
42	Laminert plakat leveres til studenttorget	1 dag	ti 01.06.10	ti 01.06.10
43	Forberede presentasjon	9 dager	fr 21.05.10	on 02.06.10
44	Presentasjon	1 dag	to 03.06.10	to 03.06.10



L Vedlegg: Faktisk prosjektplan

	Aktivitetsnavn	Varighet	Start	Slutt
1	Rapportskriving	93 dager	ma 11.01.10	on 19.05.10
2	Forprosjekt	15 dager	ma 11.01.10	fr 29.01.10
3	Arbeide med forprosjekt dokumentet	15 dager	ma 11.01.10	fr 29.01.10
4	Lære LateX	21 dager	ma 11.01.10	ma 08.02.10
5	Utvikle Webside	5 dager	ma 18.01.10	fr 22.01.10
6	Utvikle spørreundersøkelse	15 dager	ma 18.01.10	sø 07.02.10
7	Jobbe med hvilke temaer spørreundersøkelsen skal c	7 dager	ma 18.01.10	ti 26.01.10
8	Finne ut hvilke virksomheter den skal distribueres til	5 dager	ma 25.01.10	fr 29.01.10
9	Test av spørreundersøkelse	1 dag	ma 01.02.10	ma 01.02.10
10	Evaluering og endringer på spørreundersøkelse	4 dager	ti 02.02.10	sø 07.02.10
11	Levere inn forprosjekt til veileder og oppdragsgiver	1 dag	ti 26.01.10	ti 26.01.10
12	Levere inn kontrakt til veileder og oppdragsgiver	1 dag	fr 29.01.10	fr 29.01.10
13	Innleveringsfrist for forprosjekt	1 dag	fr 29.01.10	fr 29.01.10
14	Jobbe med Statusrapport	2 dager	ma 08.02.10	ti 09.02.10
15	Levere statusrapport	1 dag	ti 09.02.10	ti 09.02.10
16	Spørreundersøkelse og Dybdeintervju	49 dager	ma 18.01.10	to 25.03.10
17	Utsending av spørreundersøkelse	2 dager	ma 08.02.10	ti 09.02.10
18	Literaturstudie	40 dager	ma 11.01.10	fr 05.03.10
19	Finne kilder	8 dager	ma 18.01.10	on 27.01.10
20	Finne gjeldende lover og standarder for tema	8 dager	ti 26.01.10	to 04.02.10
21	Analysere viktige lover og standarder	9 dager	ma 08.02.10	to 18.02.10
22	Forberede dybdeintervju	15 dager	fr 19.02.10	to 11.03.10
23	Lære analyse-verktøyet "R"	11 dager	ma 22.02.10	ma 08.03.10
24	Sette seg inn i nødvendig kunnskap for videre arbeid	35 dager	ma 18.01.10	fr 05.03.10
25	Forventet svar på spørreundersøkelse	1 dag	ma 08.03.10	ma 08.03.10
26	Utføre dybdeintervju	15 dager	fr 12.03.10	to 01.04.10
27	Bearbeide data og forberede veiledning	10 dager	fr 02.04.10	to 15.04.10
28	Jobbe med Statusrapport	2 dager	fr 02.04.10	ma 05.04.10
29	Levere Statusrapport	1 dag	ma 05.04.10	ma 05.04.10
30	Påskeferie	5 dager	ma 05.04.10	fr 09.04.10
31	Skrive veiledning og gjøre klart for innlevering	28 dager	ma 12.04.10	on 19.05.10
32	Utvikle veiledning for små bedrifter	28 dager	ma 12.04.10	on 19.05.10
33	Kartlegge behov for små bedrifter	7 dager	ma 12.04.10	ti 20.04.10
34	Utvikle veiledning for mellomstore bedrifter	28 dager	ma 12.04.10	on 19.05.10
35	Kartlegge behov for mellomstore bedrifter	7 dager	ma 12.04.10	ti 20.04.10
36	Analysere data og finne de viktigste aspektene	12 dager	ma 12.04.10	ti 27.04.10
37	Vurdere struktur og oppsett for veiledning	12 dager	ma 12.04.10	ti 27.04.10
38	Forberede innlevering	9 dager	fr 07.05.10	on 19.05.10
39	Levere bachelor oppgaven til kopisentralen	1 dag	to 20.05.10	to 20.05.10
40	Levere bachelor oppgaven til studenttorget	1 dag	ti 25.05.10	ti 25.05.10
41	A3 plakat leveres til laminering	1 dag	to 27.05.10	to 27.05.10
42	Laminert plakat leveres til studenttorget	1 dag	ti 01.06.10	ti 01.06.10
43	Forberede presentasjon	9 dager	fr 21.05.10	on 02.06.10
44	Presentasjon	1 dag	to 03.06.10	to 03.06.10



M Vedlegg: Prosjektavtale

HØGSKOLEN I GJØVIK

PROSJEKTAVTALE

mellom Høgskolen i Gjøvik (HiG) (utdanningsinstitusjon),

Norsk senter for informasjonssikring (NorSIS) (oppdragsgiver), og

Lars Arne Sand, Anders Sand Fragner og Gaute Björklund Wangen

(student(er))

Avtalen angir avtalepartenes plikter vedrørende gjennomføring av prosjektet og rettigheter til anvendelse av de resultater som prosjektet frembringer:

1. Studenten(e) skal gjennomføre prosjektet i perioden fra 11/01-2010 til 25/05-2010.

   Studentene skal i denne perioden følge en oppsatt fremdriftsplan der HiG yter veiledning. Oppdragsgiver yter avtalt prosjektbistand til fastsatte tider. Oppdragsgiver stiller til rådighet kunnskap og materiale som er nødvendig for å få gjennomført prosjektet. Det forutsettes at de gitte problemstillinger det arbeides med er aktuelle og på et nivå tilpasset studentenes faglige kunnskaper. Oppdragsgiver plikter på forespørsel fra HiG å gi en vurdering av prosjektet vederlagsfritt.

2. Kostnadene ved gjennomføringen av prosjektet dekkes på følgende måte:
   - Oppdragsgiver dekker selv gjennomføring av prosjektet når det gjelder f.eks. materiell, telefon/fax, reiser og nødvendig overnatting på steder langt fra HiG. Studentene dekker utgifter for trykking og ferdigstillelse av den skriftlige besvarelsen vedrørende prosjektet.
   - Eiendomsretten til eventuell prototyp tilfaller den som har betalt komponenter og materiell mv. som er brukt til prototypen. Dersom det er nødvendig med større og/eller spesielle investeringer for å få gjennomført prosjektet, må det gjøres en egen avtale mellom partene om eventuell kostnadsfordeling og eiendomsrett.

3. HiG står ikke som garantist for at det oppdragsgiver har bestilt fungerer etter hensikten, ei heller at prosjektet blir fullført. Prosjektet må anses som en eksamensrelatert oppgave som blir bedømt av faglærer/veileder og sensor. Likevel er det en forpliktelse for utøverne av prosjektet å fullføre dette til avtalte spesifikasjoner, funksjonsnivå og tider.

4. Den totale besvarelsen med tegninger, modeller og apparatur så vel som programlisting, kildekode, disketter, taper mv. som inngår som del av eller vedlegg til besvarelsen, gis det en kopi av til HiG, som vederlagsfritt kan benyttes til undervisnings- og forskningsformål. Besvarelsen, eller vedlegg til den, må ikke nyttes av HiG til andre formål, og ikke overlates til utenforstående uten etter avtale med de øvrige parter i denne avtalen. Dette gjelder også firmaer hvor ansatte ved HiG og/eller studenter har interesser.

   Besvarelser med karakter C eller bedre registreres og plasseres i skolens bibliotek. Det legges også ut en elektronisk prosjektbesvarelse uten vedlegg på bibliotekets del av skolens Internett-sider. Dette avhenger av at studentene skriver under på en egen avtale hvor de gir biblioteket tillatelse til at deres hovedprosjekt blir gjort tilgjengelig i papir og nettutgave (jfr. Lov om opphavsrett). Oppdragsgiver og veileder godtar slik

offentliggjøring når de signerer denne prosjektavtalen, og må evt. gi skriftlig melding til studenter og dekan om de i løpet av prosjektet endrer syn på slik offentliggjøring.

5. Besvarelsens spesifikasjoner og resultat kan anvendes i oppdragsgivers egen virksomhet. Gjør studenten(e) i sin besvarelse, eller under arbeidet med den, en patentbar oppfinnelse, gjelder i forholdet mellom oppdragsgiver og student(er) bestemmelsene i Lov om retten til oppfinnelser av 17. april 1970, §§ 4-10.

6. Ut over den offentliggjøring som er nevnt i punkt 4 har studenten(e) ikke rett til å publisere sin besvarelse, det være seg helt eller delvis eller som del i annet arbeide, uten samtykke fra oppdragsgiver. Tilsvarende samtykke må foreligge i forholdet mellom student(er) og faglærer/veileder for det materialet som faglærer/veileder stiller til disposisjon.

7. Studenten(e) leverer 3 - tre - eksemplarer av oppgavebesvarelsen med vedlegg til Studenttorget. I tillegg leveres et eksemplar til oppdragsgiver. HiG kan stille til disposisjon ytterligere eksemplar(er) for oppdragsgiver mot at denne godtgjør produksjonskostnadene.

8. Denne avtalen utferdiges med et eksemplar til hver av partene. På vegne av HiG er det dekan som godkjenner avtalen.

9. I det enkelte tilfelle kan det inngås egen avtale mellom oppdragsgiver, student(er) og HiG som nærmere regulerer forhold vedrørende bl.a. eiendomsrett, videre bruk, konfidensialitet, kostnadsdekning og økonomisk utnyttelse av resultatene.

   Dersom oppdragsgiver og student(er) ønsker en videre eller ny avtale, skjer dette uten HiG som partner.

10. Når HiG også opptrer som oppdragsgiver trer HiG inn i kontrakten både som utdanningsinstitusjon og som oppdragsgiver.

11. Eventuell uenighet vedrørende forståelse av denne avtale løses ved forhandlinger avtalepartene i mellom. Dersom det ikke oppnås enighet, er partene enige om at tvisten løses av voldgift, etter bestemmelsene i tvistemålsloven av 13.8.1915 nr. 6, kapittel 32.

12. Deltakende personer ved prosjektgjennomføringen:

HiGs veileder (navn): Nils Kalstad Svendsen

Oppdragsgivers kontaktperson (navn): Tore Larsen Orderløkken

Student(er) (signatur): Lars Ståre Sand dato 28/01-2010

Gunte Wangen dato 28/1-2010

Andreas Sand Haugner dato 28/1-2010

dato

Oppdragsgiver (signatur): TO Orderløkken dato 27/1-10

Dekan (signatur): dato 28/1-2010

Revidert 11.10.07, Ivar Moe

N Vedlegg: Arbeidslogg

Timeføring

Vi brukte Excel for å føre arbeidstimer. Hvert gruppemedlem hadde et eget dokument for å føre arbeidstimer. Dokumentet var formet som bildet nedenfor viser. En side ble fylt ut pr uke. Ettersom prosjektet varte i 20 arbeidsuker (til prosjektinnlevering 20.05.2010) ble 20 slike sider fylt ut pr medlem. Siden arbeidstimer blir oppsummert på hver side, var det enkelt å holde oversikt over hvor mange arbeidstimer hvert gruppemedlem har arbeidet, samt hvor mange timer hvert gruppemedlem har brukt på de ulike temaene oppgaven besto av.

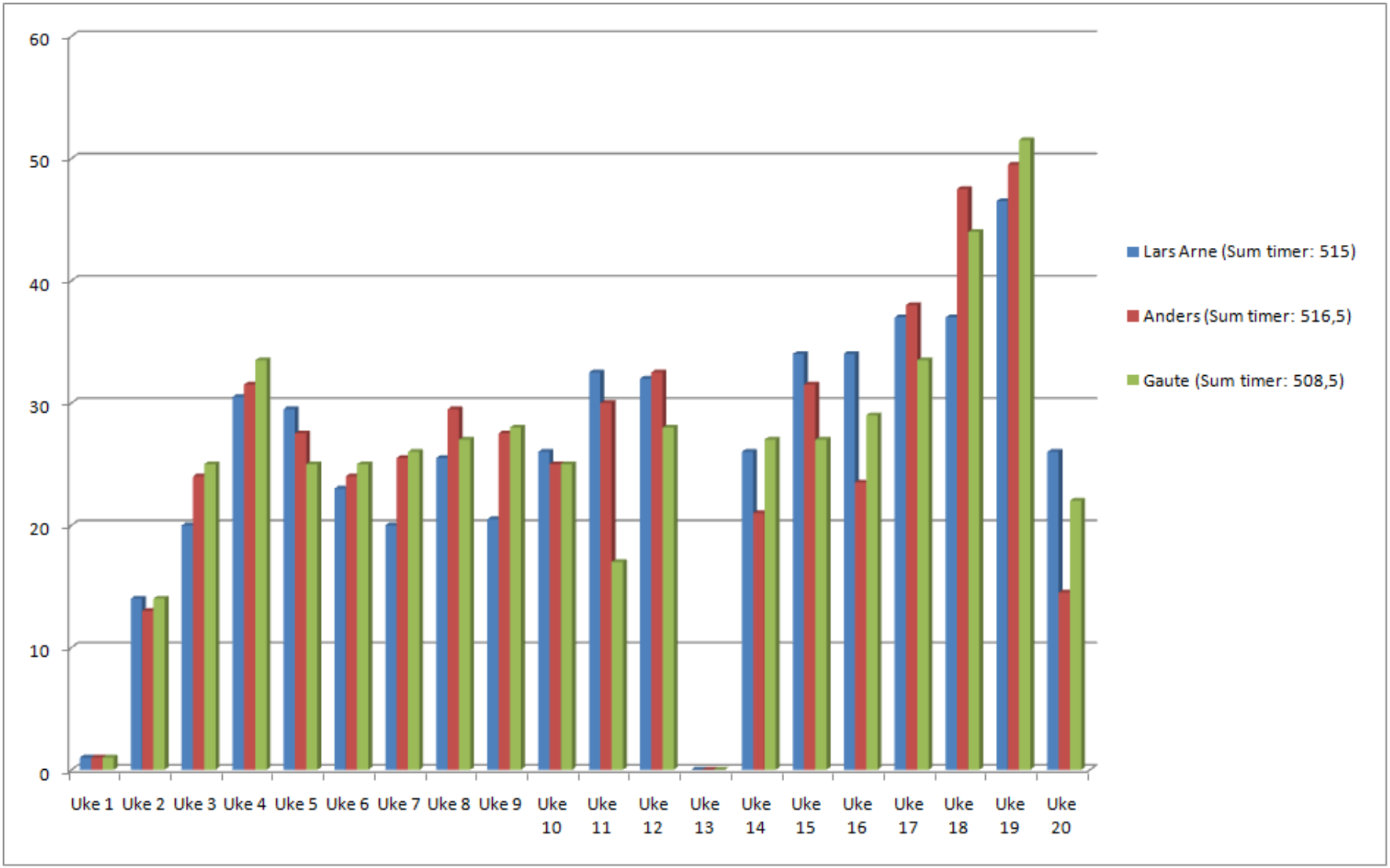
Navn: Lars Arne

Uke: 15 År: 2010

	Prosjektnr.:	Prosjektnavn:	Sum uke	Sum til nå	Mandag	Tirsdag	Onsdag	Torsdag	Fredag	Lørdag	Søndag	Kommentarer
Prosjekter	1	Bacheloroppgave	0,00	1,00								
	2	Forprosjekt	0,00	44,50								
	3	Litteraturstudie	0,00	20,00								
	4	Webside	0,00	0,00								
	5	Spørreundersøkelse	0,00	72,50								
	6	Dybdeintervju	0,00	35,00								
	7	Skriptutvikling	8,00	53,50	2,00	3,00		2,00	1,00			
	8	Statistikk	23,00	105,00	7,00	5,00		4,00	7,00			
	9	Veiledning	3,00	3,00				3,00				Workshop på veiledning.
	10											
	11											
	12											
	13											
	14											
	15											
	0											
	0											
	0											
Sum registrerte timer:			34,00	334,50	9,00	8,00	0,00	9,00	8,00	0,00	0,00	

Utdypende informasjon om arbeidstimer kan finnes her:
http://hovedprosjekter.hig.no/v2010/imt/is/hh_smb/arbeidstimer.zip

På neste side vises oversikt over arbeidsmengde pr gruppemedlem for hver uke i arbeidsperioden.


60
50
40
30
20
10
0
Uke 1
Uke 2
Uke 3
Uke 4
Uke 5
Uke 6
Uke 7
Uke 8
Uke 9
Uke 10
Uke 11
Uke 12
Uke 13
Uke 14
Uke 15
Uke 16
Uke 17
Uke 18
Uke 19
Uke 20
Lars Arne (Sum timer: 515)
Anders (Sum timer: 516,5)
Gaute (Sum timer: 508,5)

O Vedlegg: Forprosjekt

Høgskolen i Gjøvik

Forprosjekt Bachelor oppgave

Hendelseshåndtering i små og mellomstore bedrifter

Av:
Anders S. Frogner
Gaute B. Wangen
Lars Arne Sand

Veilder:
Nils Karlstad Svendsen
Oppdragsgiver:
Tore Orderløkken

Contents

List of Figures

1 Mål og Rammer

Denne delen av forprosjektet inneholder informasjon om hva som er bakgrunnen og hensikten med oppgaven. Hvilke mål som er satt og hva prosjektet skal resultere i. Den tar også for seg budsjett og rammene som er relevante for oppgaven, samt etiske og lovlige hensyn.

1.1 Bakgrunn

De fleste små og mellomstore virksomheter er veldig avhengige av IT-systemer, og at IT-systemer gjør virksomheter mer konkurransedyktige[1]. Mange lagrer mesteparten av kundedata digitalt, og skulle dette forsvinne kan det ha store konsekvenser for en virksomhet. Bruken av internett har også økt kraftig de siste årene. Virksomheter som baserer seg på kjøp og salg av varer på internett er avhengige av å ha et oppegående og pålitelig system. På grunn av dette øker risikoen for å kunne bli utsatt for forskjellige typer angrep eller sikkerhetshendelser. Dersom det skulle oppstå en sikkerhetshendelse er virksomheter avhengige av å kunne håndtere disse kjapt og effektivt. Like mye for å begrense skade, som å komme tilbake til normal drift så fort som mulig. En av betingelsene for å komme raskest mulig tilbake til normal drift er å ha en god hendelseshåndteringsplan. Hendelseshåndteringsplan er en plan som definerer hva som bør gjøres dersom en spesifikk sikkerhetshendelse inntreffer. Denne planen definerer hva som skal til for at denne planen skal aktiveres, hvilke tiltak som bør utføres og hvem som bør utføre disse. En hendelseshåndteringsplan er som regel et resultat av en hendelseshåndteringsprosess, denne prosessen består av å kartlegge verdier og risikoer, deretter klassifisere disse etter alvorlighet, for så å utvikle planer med preventive og reaktive tiltak.

1.2 Problemstilling

Etter flere års arbeid med SMBer(små og mellomstore bedrifter) har NorSIS(Norsk Senter for Informasjonssikring) fått erfare at hendelseshåndtering sjelden er en prioritet. Få bedrifter har utarbeidet hendelseshåndteringsplaner, og de som har, sliter med å implementere planene i praksis. Grunnen til dette kan være at planene er for store og detaljerte, slik at implementasjon uteblir, eller blir nedprioritert. Det er på bakgrunn av dette at oppgaven er lagd, og følgende forskningsspørsmål er opprettet:

1. I hvilken grad har virksomheter en hendelseshåndteringspolicy, eller en hendelseshåndteringspolicy de følger?

2. I hvilken grad har virksomheter opplæring på hendelseshåndtering?

3. I hvilken grad implementerer virksomheter hendelseshåndteringsplaner?

4. I hvilken grad har virksomheter rapporteringsmekanismer?

5. I hvilken grad har virksomheter oppfølging av sikkerhetshendelser?

Oppgaven vår er å bekrefte / avkrefte disse påstandene, for å oppnå dette har vi valgt å utføre en spørreundersøkelse og dybdeintervjuer, metodikken er beskrevet nærmere i seksjon 2.1 oppgavebeskrivelse.

1.3 Effektmål

En virksomhet med gode hendelseshåndteringsrutiner har økt forståelse for egne verdier og truslene den står ovenfor. I tillegg til bedre evner for å takle eventuelle sikkerhetshendelser som måtte oppstå. Ettersom oppdragsgivers arbeid går på å øke SMBers fokus på informasjonssikkerhet, vil hovedeffektmålene til prosjektet fokusere på å øke fokus på hendelseshåndtering generelt hos bedrifter, for å hjelpe bedrifter med å oppnå bedre forståelse for, og rutiner rundt hendelseshåndtering. Prosjektet har følgende effektmål:

1. Et større fokus rundt hendelseshåndtering hos SMBer.

2. En bredere oversikt over hvordan små og mellomstore bedrifter håndterer forskjellige typer sikkerhetshendelser.

3. Bedre forståelse rundt temaet hendelseshåndtering og IT sikkerhet innad i SMBer.

4. Få flere SMBer til å implementere og bruke hendelseshåndteringsrutiner.

1.4 Resultatmål

For å oppnå effektmålene satt i 1.3, og besvare forskningsspørsmålene som er satt opp, ønsker oppdragsgiver en rapport som besvarer analysen av forskningsspørsmålene, samt veiledninger som kan benyttes av SMBer for å opprette og implementere egne hendelseshåndteringsrutiner. Som resultat av rapporten:

1. Rapporten skal omhandle situasjonen i norske små og mellomstore virksomheter med tanke på hendelseshåndtering.

2. Rapporten skal være et resultat av analysen som blir gjort av spørreundersøkelsen.
3. Den skal inneholde drøftinger av funnene vi har gjort, med vekt på å besvare forskningsspørsmålene som er gitt i problembeskrivelsen.
4. Hvis analysen av spørreundersøkelsen avdekker andre relevante sider ved hendelseshåndtering, skal vi belyse disse i rapporten vår.

Som resultat av veiledningen:

1. Veiledningen skal være todelt, en for små virksomheter og en for mellomstore.
2. Veiledningen har fokus på hva som er viktig for små og mellomstore bedrifter innenfor hendelseshåndtering.
3. Veiledningen inneholder tiltak som er nødvendige i forhold til virksomhetens størrelse.
4. Den skal inneholde minimumskrav for implementering av deteksjonsverktøy og rapporteringsmekanismer.
5. Veiledningen skal gjøre implementeringen av hendelseshåndteringspolicy enklere.

1.5 Læringsmål

Oppgaven er omfattende og vil kreve mye generell kunnskap fra alle fagene vi har hatt gjennom studieløpet, men også dybdekunnskap i fag som Hendelseshåndtering, som er ekstra relevante. Vi kommer i løpet av perioden til å anvende allerede tilegnet kunnskap om systemutvikling for å best bestemme hvilken modell vi skal bruke. Vi kommer også til å bruke tilegnet kunnskap fra fagene Hendelseshåndtering og Risikostyring for å kunne vurdere forskjellige trusler, tiltak og rutiner. Denne kunnskapen vil også brukes for å kunne opprette et spørreundersøkelsesskjema. Vi vil i løpet av perioden jobbe med bacheloroppgaven og tilegne oss kunnskap om hvordan man jobber med et større prosjekt, og hvordan vi forholder oss til prosjektjobbing mot reelle virksomheter. Vi vil også anskaffe oss ny kunnskap innen hendelseshåndterings emnet for å kunne løse oppgaven på best mulig måte.

1.6 Rammer

Denne delen tar for seg rammene som er relevante for prosjektet, dette være seg kontaktpersoner, utviklingsmiljø, økonomi og tidsfrister.

1.6.1 Kontaktpersoner

Vi vil benytte kontaktnettet til oppdragsgiver under arbeid med spørreundersøkelsen. Eksterne personer som bidrar til prosjektet er Tore Orderløkken, oppdragsgiver og leder i NorSIS, og Nils Kalstad Svendsen, førsteamanuensis fra Høgskolen i Gjøvik.

1.6.2 Utviklingsmiljø

Programvare som vi skal benytte er Questback til å utføre spørreundersøkelsen, Latex til strukturering og skriving av rapporten, og siden vi muligens kommer til å handtere sensitiv informasjon, kommer vi til å anvende sikker lagring av dokument online, som blir tilbudt av skolen via Subversion.

1.6.3 Tidsfrister

Prosjektets innleveringsfrist er satt av Høgskolen i Gjøvik, og skal leveres 20.05.10 innen kl. 12.00.

1.6.4 Økonomi

Midler stilles til disposisjon fra NorSIS.

1.7 Etiske og lovlige hensyn

Siden oppgaven benytter spørreundersøkelse og dybdeintervjuer, vil det genereres mye data. Det er derfor nødvendig å drøfte hvordan data skal behandles i forhold til lovverk og beskyttelse av sensitiv data for virksomheter. Ifølge personopplysningsloven §8 kan personopplysninger bare behandles dersom den registrerte har samtykket. Det vil si at vi må få samtykke fra virksomhetene i det vi sender ut spørreundersøkelsen for at vi skal kunne lagre og behandle data. All data av sensitiv art vil bli anonymisert i rapporten, slik at det er umulig å uthente informasjon knyttet til en spesifikk virksomhet.

2 Omfang

Denne delen av forprosjektet inneholder informasjon om hvordan prosjektet skal utføres, det vil hvilke metoder som benyttes for å oppnå de ulike målene og hvorfor disse metodene er valgt. Den inneholder også informasjon om hvilke avgrensinger som er tatt i oppgaven, og begrunnelse for disse.

2.1 Oppgavebeskrivelse

Hendelseshåndtering har eksistert lenge, og det finnes mange standarder og mye faglitteratur som dekker nettopp dette[2][3]. Til tross for dette er det ikke mange virksomheter som tar hendelseshåndtering på alvor, og de virksomhetene som forsøker å implementere hendelseshåndteringsrutiner, har ofte problemer med å følge rutinene som blir satt opp[4]. Det er på bakgrunn av dette at oppgaven er utformet, og forskningsspørsmålene i seksjon 1.2 er stilt. For å besvare disse forskningsspørsmålene har vi satt opp noen hypoteser. For å ta stilling til om disse hypotesene er korrekte, er det videre utformet noen spørsmål, som vil bli brukt i spørreundersøkelsen.

- Nesten ingen virksomheter følger hendelseshåndteringspolicy, eller som har hendelseshåndteringspolicy som er tilstrekkelig.
  - Har virksomheten en policy som dekker hendelseshåndtering?
  - Dekker policyen hendelseshåndtering, og er den tilstrekkelig? Det vil si, dekker den de nødvendige aspektene for en god policy. Eksempler på dette er: omfang, roller, ansvar og støtte fra ledelsen.
- De fleste virksomheter har dårlig opplærling på hendelseshåndtering.
  - Har virksomheten opplæring på hendelseshåndtering?
  - Hvis opplæring finnes, hva slags opplæring og hvor ofte?
- De fleste virksomheter har mangelfull eller ingen implementasjon av hendelseshåndtering.
  - Har dere hendelseshåndteringsplaner?
  - Blir disse planene brukt under sikkerhetshendelser?
  - Når blir planen tatt i bruk, finnes det en 'trigger'?
  - Er ansvarsroller fordelt?
  - Er hendelseshåndteringsplanen tilstrekkelig. Det vil si, dekker den de nødvendige aspektene for en god hendelseshåndteringsplan. Eksempler på dette er: omfang, roller, ansvar, trigger, underretning, revidering.
  - Finnes det rutiner for å revidere hendelseshåndteringsplaner eller revidering etter sikkerhetshendelser?
- Generelt dårlige rapporteringsmekanismer, noe som fører til dårlig oversikt over antall sikkerhetshendelser.

  - Finnes det metoder for å registrere sikkerhetshendelser?
  - Samles sikkerhetshendelser i statistikk?
  - Rapporteres sikkerhetshendelser til ledelsen?

- Dårlig oppfølging av sikkerhetshendelser er en gjenganger i virksomhetene.
  - Dersom det oppdages en sikkerhetshendelse, gjøres det noe med den?
  - Finnes det et klart fordelt ansvar, eller konsekvenser dersom man ikke følger opp?
  - Har virksomheten vurdert hvordan sikkerhetshendelsen påvirker virksomheten?

2.2 Metodikk og kvalitetssikring

For å bekrefte/avkrefte disse hypotesene skal det utføres en spørreundersøkelse hos en rekke norske SMBer, og dybdeintervju hos noen få utvalgte. Siden spørreundersøkelsen danner grunnlaget for å analysere tilstanden hos SMBer, og ta stilling til hypotesene oppgaven baserer seg på, er det viktig at denne sendes ut tidlig og utføres korrekt. Spørreundersøkelsen vil først bli testet på noen få SMBer eller personer for å sikre at vi får tilbake svar som kan benyttes for å ta stilling til hypotesene, eller belyse andre aspekter som kan være viktige for oppgaven. Dersom denne testen viser svakheter ved spørsmål eller oppsett, vil dette endres før spørreundersøkelsen sendes ut til resten. Et annet viktig punkt er å gjøre spørreundersøkelsen attraktiv for virksomhetene slik at vi får mest mulig svar. Dette gjøres ved å sende ut et dokument sammen med spørreundersøkelsen som forklarer hensikten med undersøkelsen, samt tilby en kopi av oppgaven etter den er ferdig. Vi tror også at oppdragsgivers renomé vil øke sannsynligheten for å få svar på undersøkelsen.

Dybdeintervjuet skal utføres etter spørreundersøkelsen er utført. Grunnen til at vi ønsker å utføre dybdeintervju er for å få dekket punkter som ikke besvares av spørreundersøkelsen, i tillegg til å samle inn informasjon som kan være for detaljert og spesifikt for spørreundersøkelsen. Vi tror dybdeintervju vil øke kvaliteten på informasjonen som er samlet inn, og bidra til å gi et bedre bilde av hvordan situasjonen er i norske SMBer med fokus på hendeslseshåndtering. Denne informasjonen vil igjen bidra til å gi et bedre grunnlag for å skrive rapporten som beskriver tilstanden i norske SMBer, samt besvare hypotesene. Informasjonen vil også være betydningsfull for veiledningen som skal utvikles, siden veiledningen skal dekke de viktigste

behovene til virksomhetene. Ettersom dybdeintervju tar tid, vil dette bare utføres hos noen få utvalgte virksomheter. Vi ser for oss at dette utføres på 2-5 virksomheter, som også har deltatt på spørreundersøkelsen.

2.3 Avgrensninger

Siden oppdragsgiver hovedsaklig arbeider med informasjonssikkerhet mot små og mellomstore bedrifter, skal også prosjektet vinkles mot denne gruppen virksomheter. Ettersom små og mellomstore bedrifter(Små og mellomstore bedrifter 0-100 ansatte[6]) utgjør 99,5%[5] av virksomhetene i Norge er dette en stor målgruppe.

Hendelseshåndtering består i hovedsak av fire hovedemner: Verdi og trusselanalyse(Business Impact Analysis(BIA)), Håndtering av sikkerhetshendelser (Incident Response(IR)), Katastrofehåndtering (Disaster Recovery(DR)) og Forsetningskontinuitet (Business Continuity(BC)). Verdi og trusselanalyse består av å identifisere de viktigste ressursene i virksomheten, i tillegg til hvilke trusler som finnes og hvordan disse kan påvirke ressursene. I all hovedsak handler denne fasen om situasjonsbevisthet for sine egne ressurser og truslene som finnes. Håndtering av sikkerhetshendelser omhandler sikkerhetshendelser av ikke alvorlig grad som kan true virksomheten. Katastrofehåndtering handler om sikkerhetshendelser som kan klassifiseres som katastrofale for virksomheten. Forretningskontinuitet omhandler sikkerhetshendelser av lik alvorlighetsgrad som katastrofehåndtering, men iverksettes bare dersom omplassering/flytting/oppbygging av virksomheten på en alternativ plassering er nødvendig som en følge av sikkerhetshendelsen. Siden sikkerhetshendelser med katastrofale følger er veldig sjeldne, vil vi fokusere på de sikkerhetshendelsene som forekommer mest, og de virksomheter flest kan takle dersom de har en plan. Dette innebærer sikkerhetshendelser av lav til middels alvorlighetsgrad, altså håndtering av sikkerhetshendelser. Vi avgrenser derfor hendelseshåndtering til verdi og trusselanalyse og håndtering av sikkerhetshendelser. Slik at oppgaven får større nytteverdi for flere virksomheter, siden bare de største virksomhetene vil kunne ha ressurser til å utvikle og etterfølge omfattende katastrofehåndtering og forretningskontinuitetsplaner.

3 Prosjektorganisering

Denne delen av forprosjektet inneholder informasjon om hvordan prosjektet er organisert. Dette være seg organisering, regler, rutiner og roller for prosjektgruppen, og en beskrivelse og begrunnelse for valgt arbeidsmetodikk for organisering og gjennomgang av prosjektet.

3.1 Roller i gruppen

Leder og kontaktperson: Lars Arne Sand
Nestleder og sekretær: Anders Frogner
Webmaster og dokumentansvarlig: Gaute Bjørklund Wangen

Leder og kontaktperson vil ha ansvaret for at arbeidet blir delegert, og at tidsfrister holdes. Lederen skal også kunne ta avgjørelser når det er stor uenighet innad i gruppen. Kontaktpersonen vil være gruppen ansikt utad, all kommunikasjon fra og til andre parter skal gå igjennom kontaktpersonen. Det er da kontaktpersonens ansvar å avtale møter og lignende.
Nestleder og sekretær vil overta ansvaret til gruppeleder dersom gruppeleder ikke er tilstede. Sekretær har ansvaret for å føre logg og notater fra forskjellige møter med veileder/oppdragsgiver. Disse notatene skal føres inn og deles med alle gruppemedlemmer.
Webmaster vil ha ansvar for utvikle, samt vedlikeholde websiden. Dette innebærer å poste nyheter, oppdateringer, og lignende. Dokumentansvarlig skal sørge for at dokumenter lagres forsvarlig og at de er tilgjengelig for alle gruppemedlemmer. Dokumentansvarlig vil også ha som oppgave å ta backup av arbeidet vårt.

3.2 Grupperegler

- Man må gi beskjed tidlig dersom man ikke får gjort, eller at man ikke har fått gjort oppgaver. Slik at andre kan ta over, eller hjelpe til med oppgavene.
- Hvis gruppa føler at det er en fripassasjer, må dette tas opp med vedkommende personlig, slik at vedkommende har tid til å forbedre seg. Det kan også utstedes en skriftlig advarsel til personen det gjelder.
- Alle skal møte på møtene hver gang hvis de har mulighet, og skal fremlegge en status-/fremdriftsrapport. Hvis frister ikke overholdes skal dette tas opp med vedkommende som ikke kunne nå fristen, hvis dette skjer gjentatte ganger uten gyldig grunn må gruppa bestemme om de vil fortsette å la gruppemedlemmet være i gruppa
- Flertallet bestemmer en sak. Gjelder saken et medlem i gruppa, har ikke vedkommende stemmerett.
- Prosjektleders stemme teller dobbelt ved ellers lik stemmegivning.
- Ved fravær på felles arbeidsdager skal vedkommende melde fra helst dagen før, og samtidig ha en gyldig begrunnelse for fraværet.

3.3 Rutiner

For å få en god flyt i prosjektarbeidet er det viktig med gode rutiner. Vi har derfor satt opp noen rutiner for å sikre at arbeid blir delegert, og at en god og jevn arbeidsmengde holdes gjennom hele prosjektet. Det er i tillegg satt opp rutiner for å sikre versjonshåndtering av dokumenter.

- Felles arbeidstid er mandager, tirsdager, torsdager og fredager fra 08.00-16.00. Hvert gruppemedlem har ansvar for å logge arbeidstimer hver for seg. Ukentlig arbeidstid per medlem skal være $\tilde{3}0$ timer.
- Alle medlemmene skal føre timelister, disse skal også inneholde hva som ble arbeidet med i de førte timene.
- Subversion benyttes for versjonshåndtering. Alle dokumenter skal lastes opp på subversion.
- Gruppeleder har ansvar for å delegere arbeidsoppgaver.

3.4 Systemutviklingsmodell

Denne delen tar for seg valget av systemutviklingsmodell for oppgaven. Hvilken metode som er valgt og hvorfor, i tillegg til vurderingen av de ulike modellene, hvilken modell som ble valgt og begrunnelse for dette.

3.4.1 Metode

Det finnes mange metoder som kan benyttes for å velge systemutviklingsmodell. En metode går på å beskrive alle systemutviklingsmodellene i detalj, for deretter å gjøre en vurdering av hvilken modell som passer best. Vi føler dette blir unødvendig mye jobb, ettersom mange av modellene ikke passer til en slik oppgave. Vi har derfor valgt å bruke en elimineringsmetode, hvor vi beskriver hvilke behov prosjektet har, for deretter å eliminere modellene basert på modellenes fordeler og ulemper.

3.4.2 Valg av modell

Ved valg av systemutviklingsmodell, legger vi stor vekt på struktur og organisering. Siden oppgaven er kritisk avhengig av spørreundersøkelsen og dybdeintervjuene må tidsfristene for disse holdes. Målene som er satt for oppgaven, og hvordan disse skal oppnås er også avklart, det vil derfor ikke forekomme store endringer underveis i oppgaven. På bakgrunn av dette er det ønskelig med en modell hvor vi kan planlegge alle milepæler og detaljer i

en tidlig fase. Ettersom de sekvensielle modellene er bedre egnet for oppgaver hvor mye er klarlagt og få endringer vil forekomme, er det disse modellene som passer vårt prosjekt best. Vi ser derfor bort fra alle iterative modeller i vår vurdering av systemutviklingsmodell.

Et annet viktig aspekt vi bør legge vekt på ved valg av systemutviklingsmodell, er størrelse. Mange modeller er ment for store prosjekter hvor det er mange prosjektarbeidere. Siden vi bare er 3 stykker, utelukker vi de større modellene som f.eks RUP(Rational Unified Process).

Etter disse avgrensningene står vi igjen med tre modeller: Gjenbruksmodellen, inkrementell modell og fossefall modellen. Siden vi ikke har funnet oppgaver som likner på våres oppgave er gjenbruk av data uinteressant og gjenbruksmodellen faller dermed bort. Den inkrementelle modellen passer godt for prosjekter hvor sluttproduktet kan deles opp i inkrementer og utvikles hver for seg. Vårt prosjekt har en rapport og veiledninger som sluttprodukt, disse er avhengige av spørreundersøkelsen og dybdeintervjuene. Rapporten vil bli utviklet underveis i prosjektet og vil ikke kunne isoleres som et inkrement. Siden vi ikke kan dele opp i inkrementer vil vi heller ikke få nytteverdien til en inkrementell modell. Denne modellen faller dermed bort.

Vi står da igjen med fossefallsmodellen som beste alternativ. Dette passer bra, ettersom styrkene til fossefallsmodellen er struktur og organisering, altså de samme egenskapene som vi har behov for. En stor svakhet i denne modellen er dersom det skulle forekomme endringer. Vi anser ikke dette som noe problem ettersom målene og arbeidet er lett å kartlegge, samt at det er liten sjanse for at dette vil endre seg. Valget av modell faller dermed på fossefallsmodellen.

3.5 Statusmøter

Det er planlagt statusmøter med veileder annenhver uke, oppdragsgiver vil bli med på disse møtene. Formelle møter utover dette vil bli avtalt etter behov.

4 Risikoanalyse

Denne delen av forprosjektet inneholder en risikoanalyse av potensielle problemer som kan oppstå, hvor stor konsekvens og sannsynlighet disse vil ha, samt preventive og reaktive mottiltak.

Risiko	Alvorlighet	Sansynlighet	Tiltak
Langvarig sykdom	Middels	Lav	Ha ryddig og oversiktelig arbeidsplan, slik at andre lett kan ta over den sykes arbeid.
Svikt i maskinvare/datatap	Høy	Lav	Vi bruker subversion og lagrer alt på nett. Så vi har backup på våre Pcer og dokumentet tilgjengelige på nett.
Ikke få svar på spørreundersøkelsen	Høy	Middels	Forebyggende tiltak, vi må gjøre spørreundersøkelsen attraktiv.
Overskride prosjektets tidsfrister	Høy	Lav	Holde tidsfriter
En dropper ut av gruppa	Lav	Lav	Ha god kommunikasjon.
Ingen virksomheter stiller opp til dybdeintervju	Høy	Lav	Forebyggende tiltak. Må gjøre spørreundersøkelsen og dybdeintervjuet attraktivt å delta på.
Ikke få tilgang til standarder	Middels	Lav	Kjøpe standardene selv.
Ikke klare å utarbeide svar på hypoteser utifra svarene på spørreundersøkelsen.	Høy	Middels	Utarbeide en god spørreundersøkelse og luke ut feil eller irrelevante spm. i pilot spørreundersøkelsen.

1	Rapportskriving	93 dager	ma 11
2	Forprosjekt	15 dager	ma 11
3	Arbeide med forprosjekt dokumentet	15 dager	ma 11
4	Utvikle spørreundersøkelse	15 dager	ma 18
5	Jobbe med hvilke temaer spørreundersøkelsen skal c	7 dager	ma 18
6	Finne ut hvilke virksomheter den skal distribueres til	5 dager	ma 25
7	Test av spørreundersøkelse	1 dag	ma 01
8	Evaluering og endringer på spørreundersøkelse	4 dager	ti 02
9	Utvikle Webside	5 dager	ma 18
10	Levere inn forprosjekt til veileder og oppdragsgiver	1 dag	ti 26
11	Levere inn kontrakt til veileder og oppdragsgiver	1 dag	fr 29
12	Innleveringsfrist for forprosjekt	1 dag	fr 29
13	Jobbe med Statusrapport	2 dager	ma 08
14	Levere statusrapport	1 dag	ti 09
15	Spørreundersøkelse og Dybdeintervju	49 dager	ma 18
16	Utsending av spørreundersøkelse	2 dager	ma 08
17	Literaturstudie	40 dager	ma 11
18	Finne kilder	8 dager	ma 18
19	Finne gjeldende lover og standarder for tema	8 dager	ti 26
20	Analysere viktige lover og standarder	9 dager	ma 08
21	Forberede dybdeintervju	15 dager	fr 19
22	Sette seg inn i nødvendig kunnskap for videre arbeid	35 dager	ma 18
23	Forventet svar på spørreundersøkelse	1 dag	ma 08
24	Utføre dybdeintervju	15 dager	fr 12
25	Bearbeide data og forberede veiledning	10 dager	fr 02
26	Jobbe med Statusrapport	2 dager	fr 02
27	Levere Statusrapport	1 dag	ma 05
28	Påskeferie	5 dager	ma 05
29	Skrive veiledning og gjøre klart for innlevering	28 dager	ma 12
30	Utvikle veiledning for små bedrifter	28 dager	ma 12
31	Kartlegge behov for små bedrifter	7 dager	ma 12
32	Utvikle veiledning for mellomstore bedrifter	28 dager	ma 12
33	Kartlegge behov for mellomstore bedrifter	7 dager	ma 12
34	Analysere data og finne de viktigste aspektene	12 dager	ma 12
35	Vurdere struktur og oppsett for veiledning	12 dager	ma 12
36	Forberede innlevering	9 dager	fr 07
37	Levere bachelor oppgaven til kopisentralen	1 dag	to 20
38	Levere bachelor oppgaven til studenttorget	1 dag	ti 25
39	A3 plakat leveres til laminering	1 dag	to 27
40	Laminert plakat leveres til studenttorget	1 dag	ti 01
41	Forberede presentasion	9 dager	fr 21

Figure 1: Gantt diagrammet

5 Referanser

[1]:The impact of industry contextual factors on IT focus and the use of IT for competitive advantage, Grover S Kearns og Albert L Lederer, 7/9/2004.
[2]:ISO 18044, International Organization for Standardization, 2004.
[3]:NIST 800-34, National Institute of Standards and Technology, 2002.
[4]:Mørketallsundersøkelse fra NorSIS, NorSIS, 2006.
[5]:SSB, Statistisk sentralbyrå.
[6]:SMB definisjoner, Finansdepartementet.

P Vedlegg: Statusrapport nr 1

Statusrapport 09.02.2010

Bacheloroppgave IMT - Hendelseshåndtering i små og mellomstore bedrifter.
Anders Sand Frogner, Gaute Bjørklund Wangen, Lars Arne Sand

1. Utført i perioden

I perioden fra prosjektstart har vi jobbet med, og fullført forprosjektrapporten. Webside for prosjektet er satt opp, og blir jevnlig oppdatert. Mye av den senere tiden har gått med på å utvikle spørreundersøkelsen, samt testing, evaluering og endring av denne. Vi har også gått igjennom en vurderingsperiode for å kunne velge ut hvilke bedrifter vi skal sende spørreundersøkelsen til.

Vi har også brukt start perioden av prosjektet til å sette oss inn i, og lære oss nødvendige verktøy, som "LateX", "Subversion/Tortoise" og "R".

2. Avvik

Vi hadde opprinnelig satt en tidligere frist for når spørreundersøkelsen skulle være ferdig. Målet var å ha spørreundersøkelsen ferdig utarbeidet og sendt sent i Januar. Av kvalitetssikringsgrunner så vi oss nødt til å utsette utsendelsen til 09.02. Vi gjør opp for den litt sene utsendelsen ved å ha jobbet med generell rapportskrivning, og studert nødvendig litteratur, som forberedelse til dybdeintervju samtidig med spørreundersøkelsen. Det er av samme årsak vi utsatte test av spørreundersøkelsen et par dager.

3. Kvalitetssikring

Spørreundersøkelsen har gjennomgått flere revisjoner. Vi har hatt en testperiode hvor et testpanel bestående av NorSIS ansatte og veileder gikk igjennom spørreundersøkelsen. Basert på tilbakemeldinger fra testrunden har vi gjort forbedringer på spørreundersøkelsen.

Spørreundersøkelsen er kritisk for videre suksess i prosjektet. Vi er avhengige av å få inn tilstrekkelige svar, og svarsmengde for å kunne dra nytte av data vi samler inn. Basert på dette har kvalitetssikring hovedsakelig omhandlet denne.

4. Konklusjon

Vi ligger nå ajour med det foreløpige gantt diagrammet, og ettersom spørreundersøkelsen nå er sendt ut (09.02.2010), vil vi i en tid fremover kunne fokusere på forberedelse til dybdeintervju. Vi har satt av en måned til arbeid med dette, og vil starte med dataanalysen så fort vi begynner å få svar på spørreundersøkelsen.

Q Vedlegg: Statusrapport nr 2

Statusrapport 12.04.2010

Bacheloroppgave IMT - Hendelseshåndtering i små og mellomstore bedrifter.
Anders Sand Frogner, Gaute Bjørklund Wangen og Lars Arne Sand.

1. Utført i perioden

Vi har i denne perioden utført spørreundersøkelse og dybdeintervjuer. Spørreundersøkelsen er sendt ut, og det er mottatt tilstrekkelige antall svar. Det er også blitt gjennomført en generell statistisk analyse og korrelasjonsanalyse på denne. Dybdeintervjuene er også ferdig utført. Her har vi intervjuet 15 intervjuobjekter, og nådd målet vi satte oss. Data fra dybdeintervjuene er hentet ut, og klare for statistisk analyse.

I tillegg til disse undersøkelsene har vi begynt å skrive på rapporten, samt arbeide med veiledningene. Det er også brukt noe tid på litteraturanalyse og gjennomgang av standarder.

2. Avvik

Vi hadde opprinnelig satt en tidligere frist for utsending av spørreundersøkelsen(08/03/2010), pga. kvalitetssikringsarbeid ble denne utsatt til 09/03/2010.

Utføring av dybdeintervjuer skulle vært ferdig 01/04/2010, men ble i stedet ferdig utført 12/04/2010. Denne forsinkelsen oppsto som resultat av at mange virksomheter sa nei til å stille på dybdeintervju. Vi fikk allikevel avtalt alle intervjuene som skulle utføres før påskeferien startet, så det ble ikke brukt mye ekstra tid i forhold til det som var satt opp.

Det er planlagt at bearbeiding av data fra dybdeintervju og spørreundersøkelse skal være ferdig 15/04/2010. Dette er en for tidlig tidsfrist ettersom vi fortsatt mangler generell analyse av dybdeintervjuene, samt spesifikke analyser som ANOVA analyse av dataen fra både spørreundersøkelsen og dybdeintervjuene. Vi ser for oss at generell analyse av dybdeintervjuene blir utført i løpet av uke 15(12/04/2010-18/04/2010), mens ANOVA analyse blir utført i løpet av april.

3. Kvalitetssikring

Vi hadde møte med veileder og Bernhard Hämmerli den 01/03/2010 om metodikk for struktur og gjennomføring av dybdeintervju. Her fikk vi gode innspill om hvordan dybdeuntervju burde utføres. Det ble ellers brukt mye tid på dybdeintervju for å forsikre at vi fikk besvart de riktige spørsmålene, samt at dybdeintervjuene ble utført korrekt. Det ble også kjørt en testrunde hvor vi intervjuet gruppemedlemmer fra en annen bachelorgruppe om deres virksomhet for å forsikre oss om at spørsmålene var gode nok og beregnet tidsramme var korrekt.

Når det gjelder den statistiske analysen er det brukt en del tid på å gå gjennom faglitteraturbok, for å forsikre at analysen utføres på en korrekt måte. Her har vi også fått god hjelp av veileder.

4. Konklusjon

Vi er ferdige med all innsamling av data, og føler vi ligger à jour med vår planlagte fremdrift. Det gjenstår noe arbeid med statistisk analyse, samt utvikling av veiledning og rapport. Det er dette vi kommer til å arbeide med i tiden fremover og mot prosjektinnlevering. Dersom vi får tid håper vi også på å kunne utvide veilederen med en e-versjon, samt gjøre en dypere og grundigere statistisk analyse av dataene.